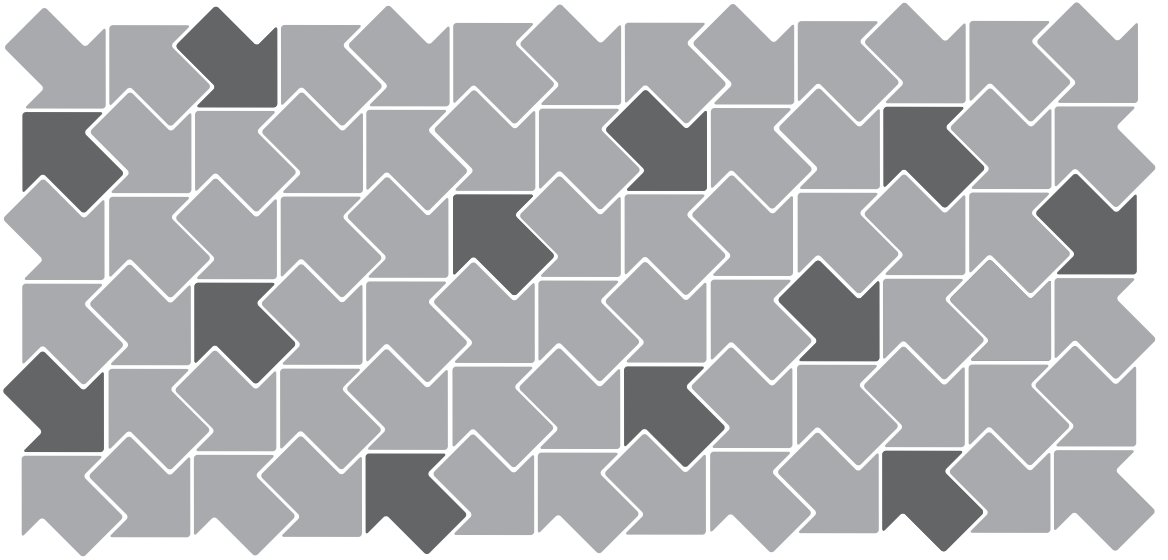
Handbuch zur Server-Konfiguration

ESX Server 3.0.1 und VirtualCenter 2.0.1



vmware®

Handbuch zur Server-Konfiguration
Überarbeitung: 20061027
Artikelnummer: VI-DEU-Q406-314

Die aktuellste technische Dokumentation erhalten Sie auf unserer Website unter

http://www.vmware.com/support/

Hier finden Sie auch die neuesten Produkt-Aktualisierungen.

Wenn Sie Kommentare oder Hinweise zu diesem Dokument haben, übermitteln Sie Ihr Feedback an:

docfeedback@vmware.com

© 2006 VMware, Inc. Alle Rechte vorbehalten. Geschützt durch mindestens eines der US-Patente Nr. 6.397.242, 6.496.847, 6.704.925, 6.711.672, 6.725.289, 6.735.601, 6.785.886, 6.789.156, 6.795.966, 6.880.022 6.961.941, 6.961.806 and 6.944.699; Patente angemeldet.

VMware, das VMware Logo und Design, Virtual SMP und VMotion sind eingetragene Marken oder Marken der VMware, Inc. in den USA und/oder anderen Ländern.

Alle anderen in diesem Dokument erwähnten Bezeichnungen und Namen sind unter Umständen markenrechtlich geschützt.

VMware, Inc.
3145 Porter Drive
Palo Alto, CA 94304
www.vmware.com

Inhalt

Einleitung 11

1 Einführung 15
- Vernetzung 15
- Speicher 16
- Sicherheit 16
- Anhänge 17

Netzwerk

2 Vernetzung 21
- Netzwerk-Konzepte 22
  - Übersicht Konzepte 22
  - Virtuelle Switches 23
  - Port-Gruppen 26
- Netzwerkdienste 27
- Anzeige der Netzwerkinformationen im VI Client 27
- Netzwerkaufgaben 29
- Konfiguration virtueller Netzwerke für virtuelle Maschinen 29
- Konfiguration des VMkernels 33
  - TCP/IP-Stapel auf Ebene der Überwachung der virtuellen 34
  - Schlussfolgerungen und Richtlinien 34
- Konfiguration der Servicekonsole 37
  - Grundlegende Konfigurationsaufgaben für die Servicekonsole 37
  - Verwendung von DHCP für die Servicekonsole 43

3 Erweiterte Netzwerkeigenschaften 45
- Erweiterte Netzwerkaufgaben 46
- Konfiguration des virtueller Switch 46
  - Eigenschaften von virtuellen Switches 46
    - Bearbeiten der Eigenschaften von virtuellen Switches 46
  - Policys für virtuelle Switches 53

Sicherheits-Policy für Layer 2 53
Traffic-Shaping-Policy 55
Policy für Lastenausgleich und Failover 57
Konfigurieren der Port-Gruppe 60
DNS und Routing 62
Einrichten von MAC-Adressen 64
Generierung von MAC-Adressen 65
Einstellen von MAC-Adressen 66
Verwendung von MAC-Adressen 66
Netzwerk-Tipps und Empfehlungen 67
Netzwerkempfehlungen 67
Einbindung von NAS-Datenträgern 67
Netzwerk-Tipps 68

4 Netzwerk-Szenarien und Problemlösung 69
Netzwerkkonfiguration für den Software iSCSI Speicher 70
Konfiguration des Netzwerks auf Blade-Servern 76
Problemlösungen 80
Fehlerbehebung bei der Vernetzung der Servicekonsole 80
Problemlösungen Netzwerkadapter-Konfiguration 82
Problemlösungen Konfiguration physischer Switches 82
Problemlösungen Port-Gruppen-Konfiguration 82

Speicher

5 Speicher - Einführung 87
Speicherkonzepte 88
Speicher - Übersicht 89
Datastores und Dateisysteme 90
Dateisystemformate 91
Speichertypen 91
Unterstützte Speicheradapter 92
Speicherzugriff durch virtuelle Maschinen 92
Anzeige der Speicherinformationen im VI Client 93
Anzeige von Datastores 94
Anzeige der Speicheradapter 95
Grundlegendes zur Benennung von Speichergeräten in der Anzeige 96
VMware Dateisystem 97
VMFS-Versionen 97

Erstellen und Vergrößern eines VMFS 98
Überlegungen beim Erstellen von VMFS 98
VMFS-Funktionen für den gemeinsamen Zugriff 99
Speichern mehrerer virtueller Maschinen auf einem VMFS-Volume 99
Gemeinsames Nutzen eines VMFS-Volumes durch mehrere ESX Server 100
Konfiguration und Verwaltung von Speicher 101

6 Speicherkonfiguration 103
Lokaler SCSI-Festplattenspeicher 104
Hinzufügen von lokalem SCSI-Speicher 104
Fibre-Channel-Speicher 106
Hinzufügen von Fibre-Channel-Speicher 108
iSCSI-Speicher 110
iSCSI-Speicher 110
iSCSI Initiatoren 110
Namenskonventionen 112
Erkennung von Speicherressourcen 112
iSCSI-Sicherheit 113
Konfigurieren von mittels Hardware ausgelöster iSCSI-Speicherung 113
Installation des iSCSI-Hardware-Initiators 114
Anzeige der Eigenschaften des iSCSI-Hardware-Initiators 114
Konfiguration eines iSCSI-Hardware-Initiators 115
Hinzufügen von hardware-initiiertem iSCSI-Speicher 120
Konfiguration von software-initiiertem iSCSI-Speicher 121
Anzeige der Eigenschaften des iSCSI-Software-Initiators 122
Konfiguration eines iSCSI-Software-Initiators 124
Hinzufügen von software-initiiertem iSCSI-Speicher 129
Neu scannen 131
NAS-Netzwerkspeicher 132
Gemeinsames Plattenspeichersystem 133
Verwendung von NFS durch virtuelle Maschinen 133
NFS-Volumes und Delegate-Benutzer virtueller Maschinen 134
Konfiguration von ESX Server zum Zugriff auf NFS-Datenträger 135
Erstellung eines NFS-basierten Datastores 135

7 Speicherverwaltung 137
Verwaltung von Datastores und Dateisystemen 138
Hinzufügen neuer Datastores 138

Entfernen bestehender Datastores 139
Bearbeiten bestehender VMFS-basierter Datastores 139
Aktualisierung von Datastores 139
Namensänderung von Datastores 140
Erweiterung von Datastores 141
Verwalten von Pfaden für Fibre-Channel und iSCSI 143
Anzeige des aktiven Multipathing-Status 145
Aktive Pfade 146
Einrichten der Multipathing-Policys für LUNs 147
Deaktivieren und Aktivieren von Pfaden 148
Einrichten des bevorzugten Pfads (Nur feste Pfadkonventionen) 149
Die `vmkfstools`-Befehle 150

8 Raw-Device-Mapping 151
Wissenswertes über Raw Device Mapping 152
Begriffe 153
Vorteile der Raw-Device-Mapping 153
Einschränkungen der Raw-Device-Mapping 156
Raw Device Mapping-Eigenschaften 156
Vergleich des virtuellen und des physischen Kompatibilitätsmodus 157
Dynamische Namensauflösung 158
Raw-Device-Mapping für Virtuelle-Maschinen-Cluster 160
Vergleich der Raw-Device-Mapping mit anderen Arten des SCSI-Gerätezugriffs 160
Verwalten zugeordneter LUNs 161
Virtual Infrastructure Client (VI Client) 161
Zuordnen einer SAN-LUN 162
Verwalten von Pfaden für eine zugeordnete Raw-LUN 163
Das `vmkfstools` Dienstprogramm 164
Dateisystemfunktionen 164

Sicherheit

9 Sicherheit für ESX Server-Systeme 167
Architektur und Sicherheitsfunktionen von ESX Server 168
Sicherheit in der Virtualisierungs-Layer 168
Sicherheit der virtuellen Maschinen 168
Sicherheit über die Servicekonsole 171
Sicherheit in der virtuellen Netzwerk-Layer 173
Sonstige Nachschlagewerke und Informationen zur Sicherheit 179

10 Absicherung der ESX Server-Konfiguration 181
Absicherung des Netzwerkes mit Firewalls 181
Firewalls in Konfigurationen mit einem VirtualCenter Server 182
Firewalls in Konfigurationen ohne VirtualCenter Server 185
TCP- und UDP-Ports für den Management-Zugriff 187
Verbindung zu einem VirtualCenter Server über eine Firewall 189
Verbindung zur Konsole der virtuellen Maschine über eine Firewall 189
Anbindung von ESX Server-Hosts über Firewalls 191
Freigeben von Firewall-Ports für unterstützte Dienste und Management-Agenten 192
Absicherung virtueller Maschinen durch VLANs 194
Sicherheitsempfehlungen für VLANs 197
Schutz durch virtuelle Switches in VLANs 199
Absicherung der Ports virtueller Switches 201
Absicherung von iSCSI-Speicher 204
Absicherung von iSCSI-Geräten über Authentifizierung 204
Schutz eines iSCSI-SANs 208

11 Authentifizierung und Anwender-Management 211
Absichern von ESX Server über Authentifizierung und Zugriffsberechtigungen 211
Anwender, Gruppen, Zugriffsberechtigungen und Rollen 213
Grundlegendes zu Anwendern 214
Grundlegendes zu Gruppen 215
Grundlegendes zu Zugriffsberechtigungen 216
Grundlegendes zu Rollen 218
Verwaltung von Anwendern und Gruppen auf ESX Server-Hosts 219
Anzeige und Export von Anwender- und Gruppeninformationen 220
Verwaltung der Anwendertabelle 222
Verwaltung der Gruppentabelle 225
Verschlüsselungs- und Sicherheitszertifikate für ESX Server 228
Hinzufügen von Zertifikaten und Änderungen der Web-Proxyeinstellungen des ESX Servers 228
Erneutes Erzeugen von Zertifikaten 233
Delegierte der virtuellen Maschine für NFS-Speicher 234

12 Sicherheit der Servicekonsole 237
Allgemeine Sicherheitsempfehlungen 238
Anmelden an der Servicekonsole 239
Konfiguration der Servicekonsolen-Firewall 240

Änderung der Sicherheitsstufe der Servicekonsole 241
Freigeben und Blockieren von Ports in der Servicekonsolen-Firewall 242
Kennwortbeschränkungen 244
Kennwort-Verwendungsdauer 245
Kennwort-Komplexität 246
Änderung des Kennwort-Plug-Ins 250
Schlüsselqualität 252
Setuid- und setgid-Anwendungen 252
setuid-Standardanwendungen 253
setgid-Standardanwendungen 255
SSH-Sicherheit 255
Sicherheitspatches und Sicherheitslücken-Scanner 257

13 Sichere Implementierungen und Sicherheits- empfehlungen 259
Sicherheitsmaßnahmen für häufig verwendete ESX Server-Implementierungen 259
Implementierung „Ein Kunde“ 259
Implementierung für mehrere Kunden mit Beschränkungen 261
Implementierung für mehrere Kunden ohne Beschränkungen 263
Empfehlungen für virtuelle Maschinen 265
Installation von Antiviren-Software. 265
Deaktivierung von Kopiervorgängen zwischen Gast-Betriebssystem und Remote-Steuerung 266
Entfernung überflüssiger Hardware-Geräte 267
Verhinderung von Flooding des ESX Server-Hosts durch Prozesse des Gast-Betriebssystems 270
Deaktivierung der Protokollierung für das Gast-Betriebssystem 271

Anhänge

A ESX-Befehle zur technischen Unterstützung 275
Andere Befehle 280

B Verwendung von `vmkfstools` 281
vmkfstools-Befehlssyntax 282
Suboption -v 283
vmkfstools-Optionen 283
Dateisystemoptionen 284
Erstellen eine VMFS-Dateisystems 284

Erweiterung eines bestehenden VMFS-3-Volumens 285
Auflistung der Attribute eines VMFS-Datenträgers 286
Upgrade von VMFS-2 auf VMFS-3 286
Optionen für virtuelle Festplatten 287
Unterstützte Festplattenformate 288
Erstellen einer virtuellen Festplatte 289
Initialisierung einer virtuellen Festplatte 289
Vergrößern einer schlanken virtuellen Festplatte 290
Löschen einer virtuellen Festplatte 290
Umbenennen einer virtuellen Festplatte 290
Klonen einer virtuellen oder Raw-Festplatte 290
Migrieren der VMware Workstation und der VMware GSX Server virtuellen Maschinen 291
Erweitern einer virtuellen Festplatte 291
Migrieren einer VMFS-2 virtuellen Festplatte auf VMFS-3 291
Anlegen einer Raw Device Mapping-Datei im virtuellen Kompatibilitätsmodus 292
Aufführen der Attribute eines RDM 292
Anlegen einer Raw Device Mapping-Datei im physischen Kompatibilitätsmodus 293
Anlegen einer Deskriptor-Datei für ein Raw-Gerät 293
Anzeige der Architektur der virtuellen Festplatte 293
Geräteoptionen 294
Scan-Adapter 294
Verwaltung der SCSI-Reservierungen von LUN 294
Beispiele für die Verwendung von vmkfstools 295
Anlegen eines neuen VMFS-3-Dateisystems 295
Hinzufügen einer Partition zu einem VMFS-3-Dateisystem 296
Neue virtuelle Festplatte erstellen 296
Klonen einer virtuellen Festplatte 296
Erstellen einer Raw-Device-Mapping 296
Scannen eines Adapters auf Änderungen 296

Stichwortverzeichnis 297

Einleitung

In diesem Vorwort werden die Inhalte des *Handbuchs zur Server-Konfiguration* beschrieben und Hinweise zu technischen und weiterführenden VMware®-Ressourcen gegeben.

In dieser Einleitung werden folgende Themen behandelt:

- „Über dieses Handbuch“ auf Seite 11
- „Technischer Support und Schulungs-Ressourcen“ auf Seite 14

Über dieses Handbuch

In diesem *Handbuch zur Server-Konfiguration* finden Sie Informationen zur Konfiguration von ESX Server (z. B. zur Erstellung von virtuellen Switches und Schnittstellen und zur Einrichtung des Netzwerkes für virtuelle Maschinen, von VMotion, von IP-Speicher und der Servicekonsole. Es behandelt außerdem die Konfiguration des Dateisystems und verschiedener Speichertypen wie z. B. iSCSI und Fibre-Channel. Zum Schutz Ihrer ESX Server-Installation findet sich außerdem in diesem Handbuch eine Abhandlung zu den Sicherheitsfunktionen, die in ESX Server integriert sind, und zu den Maßnahmen, mit denen ESX Server vor Angriffen geschützt werden können. Ferner enthalten ist eine Liste mit technischen Unterstützungsbefehlen für ESX Server und deren Entsprechung im VI Client sowie eine Beschreibung des Dienstprogramms `vmkfstools`.

Verlauf der Überarbeitung

Dieses Handbuch wird für jedes Produkt-Release überarbeitet, bzw. immer dann, wenn es notwendig ist. In einer überarbeiteten Version können sowohl kleinere als auch größere Änderungen enthalten sein. Tabelle P-1 ist der Verlauf der Überarbeitung für dieses Handbuch enthalten.

Tabelle P-1. Verlauf der Überarbeitung

Überarbeitung	Beschreibung
20060615	ESX Server 3.0 und VirtualCenter 2.0 des *Handbuchs zur Server-Konfiguration* für VMware Infrastructure 3. Dies ist die Erstausgabe dieses Handbuchs.
20060925	ESX Server 3.0.1 und VirtualCenter 2.0.1 des *Handbuchs zur Server-Konfiguration* für VMware Infrastructure 3. Diese Ausgabe enthält geringfügige Änderungen hinsichtlich der Informationen über die Speicher- und Netzwerkkonfiguration.

Zielgruppe

Dieses Handbuch richtet sich an alle Benutzer, die ESX Server 3 installieren und verwenden oder ein Upgrade durchführen möchten. Die Informationen in diesem Handbuch wurden für erfahrene Administratoren von Windows- oder Linux-Systemen geschrieben, die mit der Technologie virtueller Maschinen und Datacenter-Vorgängen vertraut sind.

Feedback zu diesem Dokument

Wenn Sie Kommentare oder Hinweise zu diesem Dokument haben, übermitteln Sie Ihr Feedback an:

docfeedback@vmware.com

VMware Infrastructure-Dokumentation

Die VMware Infrastruktur-Dokumentation besteht aus dem Dokumentationssatz für VirtualCenter und den ESX Server.

Auf den folgenden Websites haben Sie Zugriff auf die aktuellsten Versionen dieses Handbuchs und anderer Dokumentationen:

http://www.vmware.com/support/pubs

Konventionen

Tabelle P-2 sind die in diesem Handbuch verwendeten typographischen Konventionen dargestellt.

Tabelle P-2. Im Handbuch verwendete Konventionen

Schriftart	Elemente
Blau (nur online)	Querverweise und E-Mail-Adressen
Blau, Fettschrift (nur online)	Verknüpfungen
Schwarz, Fettschrift	Elemente der Benutzeroberfläche wie z. B. Schaltflächenbezeichnungen und Menüelemente
`Nicht-Proportionalschrift`	Befehle, Dateinamen, Verzeichnisse und Pfadangaben
`Nicht-Proportionalschrift, fett`	Benutzereingabe
Kursiv	Titel von Dokumentationen, Glossarbegriffe und gelegentliche Hervorhebung
< Name >	Namen von Variablen und Parametern

In Grafiken verwendete Abkürzungen

In den Grafiken in diesem Handbuch werden die Abkürzungen verwendet, die in Tabelle P-3 aufgeführt sind.

Tabelle P-3. Abkürzungen

Abkürzung	Beschreibung
VC	VirtualCenter
VI	Virtual Infrastructure Client
Server	VirtualCenter Server
Datenbank	VirtualCenter-Datenbank
Host*n*	Die von VirtualCenter verwalteten Hosts
VM#	Die virtuellen Maschinen auf einem verwalteten Host
Anwender#	Anwender mit Zugriffsrechten
dsk#	Speicherfestplatte für den verwalteten Host
Datenspeicher	Speicher für den verwalteten Host
SAN	Datastore des Typs Storage Area Network, den sich verwaltete Hosts teilen
tmplt	Template

Technischer Support und Schulungs-Ressourcen

In den folgenden Abschnitten werden die verschiedenen zur Verfügung stehenden technischen Hilfsmaterialien beschrieben.

Selbsthilfe-Support

Mithilfe des VMware Technologienetzwerks (VMTN) können Sie Tools zur Selbsthilfe und technische Informationen herunterladen:

- Produktinformationen – **http://www.vmware.com/products/**
- Technologieinformationen – **http://www.vmware.com/vcommunity/technology**
- Dokumentation – **http://www.vmware.com/support/pubs**
- VMTN-Wissensbasis – **http://www.vmware.com/support/kb**
- Diskussionsforen – **http://www.vmware.com/community**
- Anwendergruppen – **http://www.vmware.com/vcommunity/usergroups.html**

Weitere Informationen zum VMware Technologienetzwerk finden Sie unter **http://www.vmtn.net**.

Online- und Telefon-Support

Im Online-Support können Sie technische Unterstützung anfordern, Ihre Produkt- und Vertragsdaten abrufen und Ihre Produkte registrieren. Weitere Informationen finden Sie unter **http://www.vmware.com/support**.

Kunden mit entsprechenden Verträgen für den Telefon-Support erhalten auf diese Weise die schnellste Hilfe bei Problemen höchster Priorität. Weitere Informationen finden Sie unter **http://www.vmware.com/support/phone_support.html**.

Support-Angebote

Hier finden Sie Informationen darüber, wie die Support-Angebote von VMware Ihnen beim Meistern Ihrer Aufgaben helfen können. Weitere Informationen finden Sie unter **http://www.vmware.com/support/services**.

VMware-Ausbildungsdienstleistungen

VMware Kurse umfassen umfangreiche Praxisübungen, Fallstudienbeispiele und Schulungsunterlagen, die zur Verwendung als Nachschlagewerke bei der praktischen Arbeit vorgesehen sind. Weitere Informationen über VMware-Schulungstleistungen finden Sie unter **http://mylearn1.vmware.com/mgrreg/index.cfm**.

1 Einführung

Das *Handbuch zur Server-Konfiguration* beschreibt die Aufgaben, die Sie zur Konfiguration des ESX Server-Hostnetzwerks, des Speichers und der Sicherheitsfunktionen durchführen müssen. Außerdem enthält es Übersichten, Empfehlungen und Grundlagenerläuterungen, die Ihnen beim Verständnis dieser Aufgaben und bei der Implementierung eines ESX Server-Hosts, der Ihren Anforderungen entspricht, helfen. Lesen Sie jedoch vor der Lektüre des *Handbuchs zur Server-Konfiguration* die *Einführung in die virtuelle Infrastruktur*. Dort finden Sie eine Übersicht über die Systemarchitekturen und die physischen und virtuellen Geräte, aus denen das System einer virtuellen Infrastruktur besteht.

Diese Einführung fasst den Inhalt dieses Handbuchs zusammen, um Ihnen die Suche nach den Informationen, die Sie benötigen, zu erleichtern. Dieses Handbuch umfasst folgende Themen:

- Netzwerkkonfiguration für ESX Server
- Speicherkonfiguration für ESX Server
- Sicherheitsfunktionen von ESX Server
- Befehle für ESX
- Der Befehl `vmkfstools`

Vernetzung

Die Kapitel zu ESX Server Netzwerken bieten Ihnen ein grundlegendes Verständnis der physischen und virtuellen Netzwerkkonzepte, eine Beschreibung der Basisaufgaben, die Sie erfüllen müssen, um die Netzwerkanschlüsse Ihres ESX Server-Hosts herzustellen, sowie eine Besprechung der erweiterten Netzwerkthemen und -aufgaben. Der Netzwerkabschnitt enthält folgende Kapitel:

- **„Vernetzung“** – Stellt Netzwerkkonzepte vor und führt durch Routineaufgaben, die zur Konfiguration eines Netzwerkes auf dem ESX Server-Host notwendig sind.
- **„Erweiterte Netzwerkeigenschaften“** – Behandelt erweiterte Netzwerkaufgaben, wie zum Beispiel die Einrichtung von MAC-Adressen, die Bearbeitung von virtuellen Switches und Ports und DNS-Routing. Außerdem enthält es Tipps, wie die Netzwerkkonfiguration effizienter gestaltet werden kann.
- **„Netzwerk-Szenarien und Problemlösung“** – Beschreibt die allgemeine Netzwerkkonfiguration und Problemlösungsszenarios.

Speicher

Das Themengebiet „Speicher“ für ESX Server beschreibt die Grundlagen zu Speichern, die grundlegenden Schritte zur Konfiguration und Verwaltung der Speicher des ESX Server-Hosts sowie die Einstellung der Raw-Device-Mapping. Der Abschnitt „Speicher“ enthält folgende Kapitel:

- **„Speicher - Einführung“** – Stellt die Speichertypen vor, die für den ESX Server-Host konfiguriert werden können.
- **„Speicherkonfiguration“** – Erläutert die Konfiguration von lokalem SCSI-Speicher, Fibre-Channel-Speicher und iSCSI-Speicher. Hier werden auch VMFS-Speicher und an das Netzwerk angebundene Speicher behandelt.
- **„Speicherverwaltung“** – Erläutert die Verwaltung von bestehenden Datastores und der Dateisysteme, aus denen die Datastores bestehen.
- **„Raw-Device-Mapping“** – Behandelt die Raw-Device-Mapping, die Konfiguration dieses Speichertyps und die Verwaltung dieser Raw-Device-Mapping durch die Einrichtung von Multipathing, Failover usw.

Sicherheit

Das Themengebiet „Sicherheit“ für ESX Server beschreibt die Sicherheitsfunktionen, die von VMware in ESX Server integriert wurden, sowie die Maßnahmen, durch die Sie den ESX Server-Host vor Gefahren schützen können. Zu diesen Maßnahmen gehören Firewalls, die Effektivierung von Sicherheitsfunktionen und virtuellen Switches sowie die Einrichtung von Anwenderauthentifizierung und Anwenderrechten. Der Sicherheitsabschnitt enthält folgende Kapitel:

- **„Sicherheit für ESX Server-Systeme“** – Stellt die ESX Server-Funktionen vor, mit denen Sie die Umgebung für Ihre Daten sichern können, und gibt eine sicherheitsbezogene Übersicht über den Systemaufbau.
- **„Absicherung der ESX Server-Konfiguration“** – Erläutert die Konfiguration von Firewall-Ports für ESX Server-Hosts und VMware VirtualCenter, die Verwendung von virtuellen Switches und VLANs zur Absicherung der Netzwerkisolierung für virtuelle Maschinen und die Absicherung von iSCSI-Speicher.

- **„Authentifizierung und Anwender-Management“** – Erläutert die Einrichtung von Anwendern, Gruppen, Zugriffsrechten und Rollen zur Steuerung des Zugriffs auf ESX Server-Hosts und VirtualCenter. Es behandelt auch die Verschlüsselung und delegierte Anwender.
- **„Sicherheit der Servicekonsole“–** Behandelt die Sicherheitsfunktionen der Servicekonsole und die Konfiguration dieser Funktionen.
- **„Sichere Implementierungen und Sicherheits- empfehlungen“–** Führt einige Beispiel-Systeme auf, um zu verdeutlichen, welche Probleme bei der Implementierung von ESX Servers beachtet werden müssen. In diesem Kapitel finden Sie außerdem weitere Hinweise zur Verbesserung der Sicherheit von virtuellen Maschinen.

Anhänge

Das *Handbuch zur Server-Konfiguration* hat zwei Anhänge, in denen Sie spezielle Informationen finden, die bei der Konfiguration von ESX Server-Hosts hilfreich sein können.

- **„ESX-Befehle zur technischen Unterstützung“** – Behandelt die Konfigurationsbefehle für ESX Server, die über eine Befehlszeilenshell wie SSH eingegeben werden können. Zwar stehen Ihnen diese Befehle zur Verfügung, es handelt sich jedoch dabei nicht um eine Programmierschnittstelle, über die Skripte erstellt werden können. Diese Befehle können sich ändern. VMware unterstützt keine Anwendungen und Skripte, die auf Konfigurationsbefehlen für ESX Server beruhen. In diesem Anhang finden Sie die entsprechenden Befehle für Client der virtuellen VMware Infrastruktur (VI Client).
- **„Verwendung von vmkfstools“** – Behandelt das Dienstprogramm `vmkfstools`, mit dem Sie Verwaltungs- und Migrationsaufgaben für iSCSI-Festplatten durchführen können.

Netzwerk

Vernetzung 2

In diesem Kapitel werden die Netzwerkgrundlagen für ESX Server-Umgebungen sowie die Einrichtung und Konfiguration von Netzwerken in virtuellen Infrastrukturen erläutert.

Mit dem Virtual Infrastructure (VI) Client können Sie eine Netzwerkanbindung herstellen. Dabei gibt es drei Kategorien, die die drei Typen von Netzwerkdiensten widerspiegeln:

- Virtuelle Maschinen
- VMkernel
- Servicekonsole

In diesem Kapitel werden folgende Themen behandelt:

- „Netzwerk-Konzepte“ auf Seite 22
- „Netzwerkdienste“ auf Seite 27
- „Anzeige der Netzwerkinformationen im VI Client“ auf Seite 27
- „Netzwerkaufgaben“ auf Seite 29
- „Konfiguration virtueller Netzwerke für virtuelle Maschinen“ auf Seite 29
- „Konfiguration des VMkernels“ auf Seite 33
- „Konfiguration der Servicekonsole“ auf Seite 37

Netzwerk-Konzepte

Es sind bestimmte Grundlagen notwendig, um virtuelle Netzwerke vollständig zu verstehen. Wenn Sie bisher noch nicht mit ESX Server 3.0 gearbeitet haben, empfiehlt VMware Ihnen dringend die Lektüre dieses Abschnittes.

Übersicht Konzepte

Ein *physisches Netzwerk* ist ein Netzwerk von physischen Computern, die so miteinander verbunden sind, dass sie untereinander Daten empfangen und versenden können. VMware ESX Server wird auf einem physischen Computer ausgeführt.

Ein *virtuelles Netzwerk* ist ein Netzwerk von virtuellen Computern (virtuellen Maschinen), die auf einem einzigen physischen Computer ausgeführt werden. Sie sind logisch miteinander verbunden, sodass sie untereinander Daten empfangen und versenden können. Virtuelle Maschinen können an die virtuellen Netzwerke angeschlossen werden, die Sie beim Hinzufügen von Netzwerken erstellen. Jedes einzelne virtuelle Netzwerk verfügt über einen virtuellen Switch. Ein virtuelles Netzwerk kann an ein physisches Netzwerk angeschlossen werden, indem mindestens ein physischer Ethernet-Adapter (auch Uplink-Adapter genannt) dem virtuellen Switch des virtuellen Netzwerks zugewiesen wird. Wenn dem virtuellen Switch kein Uplink-Adapter zugewiesen wurden, ist der Datenverkehr im virtuellen Netzwerk auf den physischen Hostcomputer beschränkt. Wenn dem virtuellen Switch mindestens ein Uplink-Adapter zugewiesen wurde, können die virtuellen Maschinen, die an dieses virtuelle Netzwerk angeschlossen sind, auch auf die physischen Netzwerke zugreifen, die an den Uplink-Adapter angeschlossen sind.

Ein *physischer Ethernet-Switch* verwaltet den Netzwerkdatenverkehr zwischen den Computern auf dem physischen Netzwerk. Ein Switch verfügt über mehrere Ports. Jeder dieser Ports kann an einen anderen Computer oder Switch im Netzwerk angeschlossen sein. Jeder Port kann je nach Bedarf des angeschlossenen Computers so konfiguriert werden, dass er sich auf eine bestimmte Art verhält. Der Switch stellt fest, welche Hosts an welche seiner Ports angeschlossen sind, und verwendet diese Informationen, um Daten an den entsprechenden richtigen physischen Computer weiterzuleiten. Switches bilden den Kern eines physischen Netzwerks. Es können mehrere Switches zusammengeschlossen werden, um größere Netzwerke zu bilden.

Ein virtueller Switch, ein sog. *vSwitch*, funktioniert ähnlich wie ein physischer Ethernet-Switch. Er weiß, welche virtuellen Maschinen logisch an welche virtuellen Ports angeschlossen sind, und verwendet diese Informationen, um Daten an die entsprechende richtige virtuellen Maschine weiterzuleiten. Ein vSwitch kann über physische Ethernet-Adapter (auch Uplink-Adapter) an physische Switches angeschlossen werden, um virtuelle und physische Netzwerke zu verbinden. Diese Verbindung ähnelt der Vernetzung von physischen Switches zur Bildung von größeren Netzwerken. Obwohl ein vSwitch ähnlich wie ein physischer Switch funktioniert, verfügt er nicht über alle erweiterten Funktionsmerkmale eines physischen Switches. Weitere Informationen zu vSwitches finden Sie unter „Virtuelle Switches“ auf Seite 23.

Eine *Port-Gruppe* legt Port-Konfigurationsoptionen wie z. B. Bandbreitenbeschränkungen oder VLAN-Tagging-Policys für jeden Port in der Port-Gruppe fest. Netzwerkdienste werden über Port-Gruppen an vSwitches angeschlossen. Die Port-Gruppen definieren, wie eine Verbindung über den vSwitch an das physische Netzwerk vorgenommen wird. Normalerweise wird einem vSwitch mindestens eine Port-Gruppe zugewiesen. Weitere Informationen zu Port-Gruppen finden Sie unter „Port-Gruppen“ auf Seite 26.

NIC-Teaming tritt auf, wenn einem vSwitch mehrere Uplink-Adapter zugewiesen werden, um ein Team zu bilden. Ein Team kann entweder den Datenverkehr zwischen dem physischen und dem virtuellen Netzwerk auf einige oder alle NICs des Teams aufteilen oder als passiver Failover im Falle einer Hardware-Störung oder eines Netzwerkausfalls dienen.

Mit *VLANs* kann ein einzelnes physisches LAN-Segment weiter aufgeteilt werden, sodass Port-Gruppen derart voneinander isoliert werden, als befänden sie sich in unterschiedlichen physischen Segmenten. Der Standard hierfür ist 802.1Q.

Der *VMkernel TCP/IP-Networking-Stack* unterstützt iSCSI, NFS und VMotion. Virtuelle Maschinen führen Ihre eigenen System- TCP/IP-Stapel aus und verbinden sich auf Ebene des Ethernets über virtuelle Switches mit dem VMkernel. Zwei neue Funktionen unter ESX Server 3, iSCSI und NFS, werden in diesem Kapitel als *IP-Speicher* bezeichnet. IP-Speicher bezeichnet jedwede Art von Speicher, der auf TCP/IP-Netzwerkkommunikation beruht. iSCSI kann als Datenspeicher für virtuelle Maschinen verwendet werden; NFS kann als Datenspeicher für virtuelle Maschinen oder für die direkte Einbindung von `.ISO`-Dateien, die dann von der virtuellen Maschine als CD-ROMs erkannt werden, verwendet werden.

HINWEIS In den Netzwerkkapiteln wird beschrieben, wie das Netzwerk für iSCSI und NFS eingerichtet wird. Informationen zur Konfiguration des Speichers von iSCSI und NFS finden Sie in den Kapiteln zum Speicher.

Mit der *Migration mit VMotion* kann eine aktivierte virtuelle Maschine von einem ESX Server-Host auf einen anderen übertragen werden, ohne dass die virtuelle Maschine her-untergefahren werden muss. Für die optionale VMotion-Funktion ist ein eigener Lizenzschlüssel notwendig.

Virtuelle Switches

Mit dem Virtual Infrastructure (VI) Client können Sie isolierte Netzwerkgeräte erstellen, die virtuelle Switches (vSwitches) genannt werden. Ein vSwitch kann Datenverkehr intern zwischen virtuellen Maschinen und zwischen virtuellen Maschinen und externen Netzwerken steuern.

HINWEIS Sie können auf einem einzigen Host höchstens 248 vSwitches anlegen.

Mit virtuellen Switches können Sie die Bandbreite mehrerer Netzwerkadapter kombinieren und den Datenverkehr darauf verteilen. Sie können auch konfiguriert werden, um physischen NIC-Failover zu gewährleisten.

Ein vSwitch täuscht einen physischen Ethernet-Switch vor. Die Standardanzahl der logischen Ports auf einem vSwitch ist 56. Mit ESX Server 3.0 können jedoch vSwitches mit bis zu 1016 Ports erstellt werden. An jeden dieser Ports können Sie einen Netzwerkadapter einer virtuellen Maschine anschließen. Jeder Uplink-Adapter, der einem vSwitch zugewiesen wurde, verwendet einen Port. Jeder logische Port auf dem vSwitch gehört zu einer Port-Gruppe. Jedem vSwitch kann mindestens eine Port-Gruppe zugewiesen werden. Weitere Informationen finden Sie unter „Port-Gruppen“ auf Seite 26.

Bevor der Netzwerkzugriff der virtuellen Maschinen konfiguriert werden kann, muss mindestens ein vSwitch erstellt worden sein. Wenn zwei oder mehr virtuelle Maschinen an den gleichen vSwitch angeschlossen sind, wird der Netzwerkdatenverkehr zwischen diesen virtuellen Maschinen lokal gesteuert. Wenn ein Uplink-Adapter dem vSwitch hinzugefügt ist, kann jede virtuelle Maschine auf das externe Netzwerk zugreifen, mit dem der Adapter verbunden ist. Dies ist unter Abbildung 2-1 angezeigt.

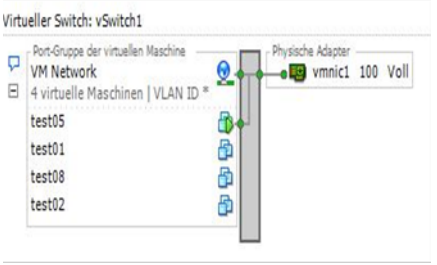


Abbildung 2-1. Verbindungen der virtuellen Switches

Im VI Client werden die Einzelheiten des ausgewählten vSwitch als interaktives Diagramm dargestellt, wie in Abbildung 2-2 angezeigt. Die wichtigsten Informationen zu allen vSwitches werden immer angezeigt.

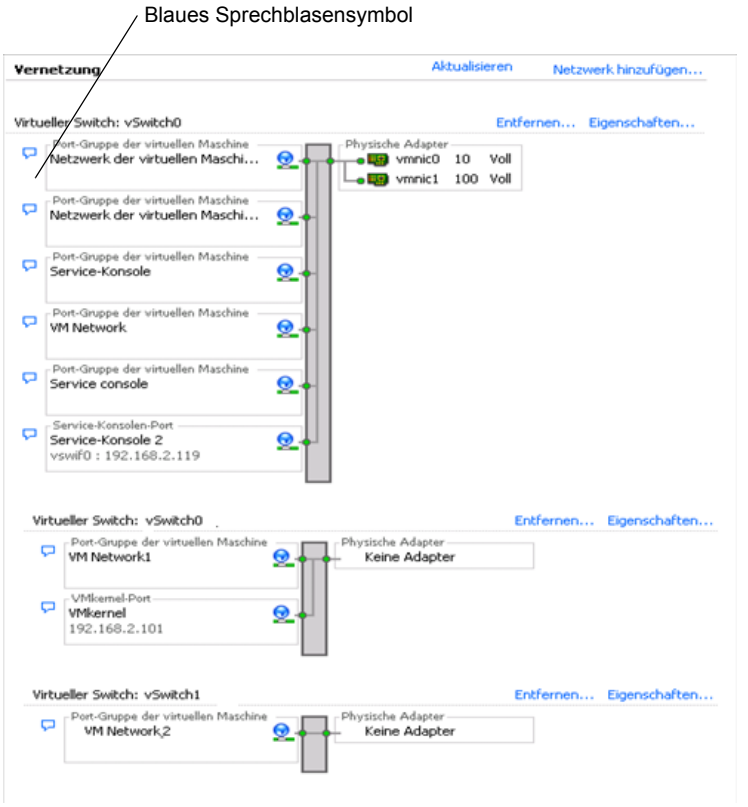


Abbildung 2-2. Interaktives Diagramm des virtuellen Switch

Klicken Sie auf das blaue Sprechblasensymbol, um sich selektiv weitere detailliertere Informationen anzeigen zu lassen.

Ein Popup-Fenster verweist auf die detaillierten Eigenschaften, wie in Abbildung 2-3 dargestellt.

Abbildung 2-3. Detaillierte Eigenschaften des virtuellen Switch

Port-Gruppen

Port-Gruppen vereinen mehrere Ports unter einer gemeinsamen Konfiguration und bieten so einen stabilen Ankerpunkt für virtuelle Maschinen, die an bezeichnete Netzwerke angeschlossen sind. Jede Port-Gruppe wird durch eine Netzwerkbezeichnung ausgewiesen, die für den vorliegenden Host einzigartig ist. Eine VLAN-ID, die den Datenverkehr der Port-Gruppe auf ein logisches Ethernet-Segment im physischen Netzwerk beschränkt, kann optional zugewiesen werden.

HINWEIS Sie können auf einem einzigen Host höchstens 512 Port-Gruppen anlegen.

Bezeichnete Netzwerke sind nur dann richtig konfiguriert, wenn alle Port-Gruppen, die die gleiche Netzwerkbezeichnung verwenden, den gleichen Datenverkehr sehen können. Da ein VLAN die Sichtbarkeit in einem physischen Netzwerk einschränken kann, ist es ggf. notwendig, die Netzwerkbezeichnung und die VLAN-ID-Steuerung abzugleichen, wenn eine der beiden geändert werden. Eine VLAN-ID kann von mehreren Port-Gruppen verwendet werden.

HINWEIS Damit eine Port-Gruppe die Port-Gruppen erreichen kann, die sich auf anderen VLANs befinden, müssen Sie die VLAN-ID auf 4095 einstellen.

Netzwerkdienste

Bei ESX Server müssen zwei Typen von Netzwerkdiensten aktiviert werden:

- Virtuelle Maschinen mit dem physischen Netzwerk verbinden
- Anschluss der VMkernel-Dienste (zum Beispiel NFS, iSCSI oder VMotion) an das physische Netzwerk

Die Servicekonsole, auf der die Verwaltungsdienste ausgeführt werden, wird automatisch während der Installation von ESX Server eingerichtet.

Anzeige der Netzwerkinformationen im VI Client

Der VI Client zeigt sowohl die allgemeinen Netzwerkinformationen als auch solche Informationen an, die den Netzwerkadaptern eigen sind.

Gehen Sie wie folgt vor, um die Netzwerkinformationen auf dem VI Client anzuzeigen

1. Melden Sie sich am VMware VI Client an und wählen Sie den Server aus dem Inventar aus.

   Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

2. Klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Netzwerk**.

Das Netzwerk-Fenster zeigt die folgenden Informationen an, wie in Abbildung 2-4 dargestellt:

- Virtuelle Switches
- Adapterinformationen zu allen Adaptern
  - Verbindungsstatus
  - Nenngeschwindigkeit und Duplex
- Servicekonsolen- und VMkernel-TCP/IP-Dienste
  - IP-Adresse
- Servicekonsole
  - Name des virtuellen Geräts
- Virtuelle Maschinen
  - Betriebsstatus
  - Verbindungsstatus
- Port-Gruppe
  - Netzwerkbezeichnung – für alle drei Typen der Port-Konfiguration einheitlich

- Anzahl der konfigurierten virtuellen Maschinen
- VLAN-ID, falls vorhanden – für alle drei Typen der Port-Konfiguration einheitlich

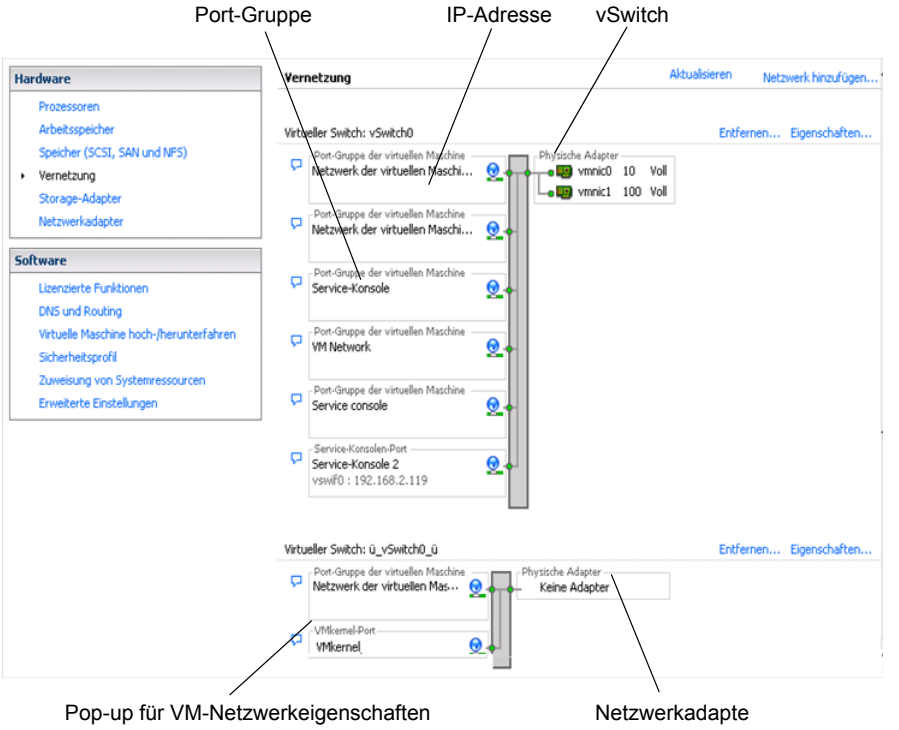


Abbildung 2-4. Allgemeine Netzwerkinformationen

Gehen Sie wie folgt vor, um die Netzwerk-Adapterinformationen auf dem VI Client anzuzeigen

1 Melden Sie sich am VMware VI Client an und wählen Sie den Server aus dem Inventar aus.

Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend auf **Netzwerkadapter**.

Das Netzwerk-Adapter-Fenster zeigt die folgenden Informationen an:

- **Gerät** – Gerätename des Netzwerkadapters
- **Geschwindigkeit** – Tatsächliche Geschwindigkeit und Duplex des Netzwerkadapters

- **Konfiguriert** – Konfigurierte Geschwindigkeit und Duplex des Netzwerkadapters
- **vSwitch** – vSwitch, dem der Netzwerkadapter zugeordnet ist
- **Netzwerke** – IP-Adressen, auf die der Netzwerkadapter zugreifen kann

Netzwerkaufgaben

In diesem Kapitel wird die Ausführung der folgenden Netzwerkaufgaben beschrieben

- „Erstellung eines virtuellen Netzwerkes für eine virtuelle Maschine“ auf Seite 30
  - Einrichtung einer Verbindungsart für eine virtuelle Maschine.
  - Hinzufügen eines virtuellen Netzwerks zu einem neuen oder einem bestehenden virtuellen Switch.
  - Konfiguration der Netzwerkbezeichnung und der Verbindungseinstellungen für die VLAN-ID.
- „Einrichtung von VMkernel“ auf Seite 34
  - Einrichtung der Verbindungsart für das VMkernel.
  - Hinzufügen eines virtuellen Netzwerks zu einem neuen oder einem bestehenden virtuellen Switch.
  - Konfiguration der Verbindungseinstellungen für die Netzwerkbezeichnung, die VLAN-ID, TCP/IP und Gateway.
- „Konfiguration der Netzwerk-Servicekonsole“ auf Seite 38
  - Einrichtung einer Verbindungsart für die Servicekonsole.
  - Hinzufügen eines virtuellen Netzwerks zu einem neuen oder einem bestehenden virtuellen Switch.
  - Konfiguration der Verbindungseinstellungen für die Netzwerkbezeichnung, die VLAN-ID, DHCP/Statische IP und die Gateway.
- „Einstellung der Standard-Gateway“ auf Seite 41
- „Anzeige von Servicekonsoleninformationen“ auf Seite 43

Konfiguration virtueller Netzwerke für virtuelle Maschinen

Der VI Client **Assistent zum Hinzufügen von Netzwerken** leitet Sie durch die Schritte, die zur Erstellung eines virtuellen Netzwerks für eine virtuelle Maschine notwendig sind. Dazu gehören:

- Einrichtung einer Verbindungsart für eine virtuelle Maschine

- Hinzufügen eines virtuellen Netzwerks zu einem neuen oder einem bestehenden vSwitch
- Konfiguration der Verbindungseinstellungen für die Netzwerkbezeichnung und die VLAN-ID

Bedenken Sie beim Einrichten von Netzwerken mit virtuellen Maschinen, ob sie die virtuellen Maschinen des Netzwerks zwischen ESX Server-Hosts migrieren möchten. Falls ja, stellen Sie sicher, dass sich beide Hosts in derselben Broadcast-Domäne befinden, also im selben Layer 2-Subnet.

ESX Server unterstützt die Migration virtueller Maschinen zwischen Hosts unterschiedlicher Broadcast-Domänen deshalb nicht, weil eine migrierte virtuelle Maschine möglicherweise Systeme und Ressourcen benötigen könnte, auf die sie aufgrund der Verschiebung auf ein separates Netzwerk keinen Zugriff mehr hätte. Selbst wenn Ihre Netzwerkkonfiguration als HV-Umgebung eingerichtet ist oder intelligente Switches enthält, die in der Lage sind, dem Bedarf einer virtuellen Maschine auch über verschiedene Netzwerke hinweg zu entsprechen, könnte es sein, dass es in der ARP-Tabelle zu Verzögerungen bei der Aktualisierung und der Wiederaufnahme des Netzwerkverkehrs der virtuellen Maschine kommt.

Erstellung eines virtuellen Netzwerkes für eine virtuelle Maschine

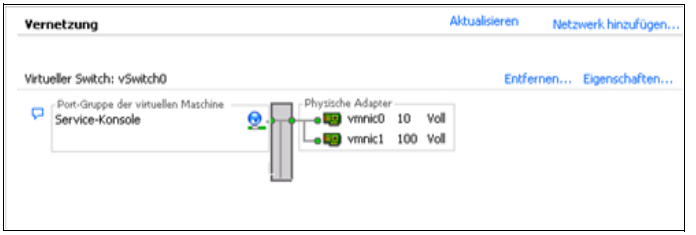
1 Melden Sie sich am VMware VI Client an und wählen Sie den Server aus dem Inventar aus.

  Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Netzwerk**.

3 Klicken Sie auf der rechten Bildschirmseite auf **Netzwerk hinzufügen**.

  Die virtuellen Switches werden als Übersicht mit Details angezeigt.



4 Klicken Sie auf die Registerkarte **Netzwerk hinzufügen** aus der Registerkarte **Konfiguration**.

  Der **Assistent zum Hinzufügen von Netzwerken** wird angezeigt.

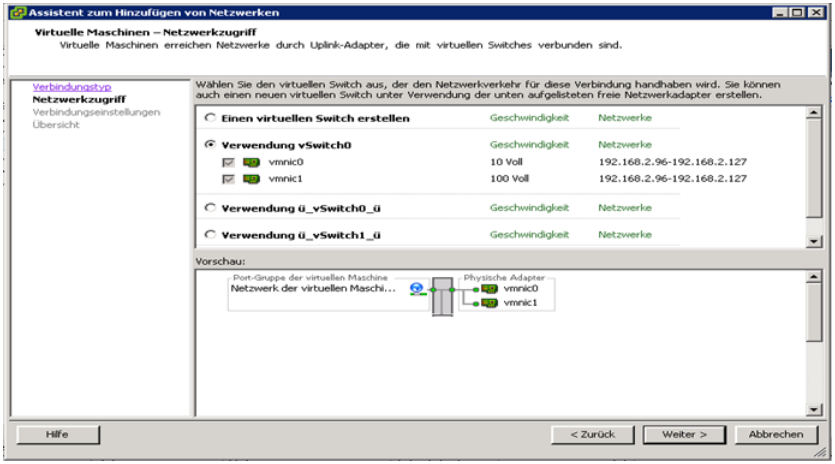
HINWEIS Der **Assistent zum Hinzufügen von Netzwerken** wird auch für neue Ports und Port-Gruppen verwendet.

5 Akzeptieren Sie die Standard-Verbindungsart **Virtuelle Maschinen**.

Durch die Auswahl der Option **Virtuelle Maschinen** können Sie ein bezeichnetes Netzwerk hinzufügen, das den Datenverkehr im Netzwerk der virtuellen Maschinen verarbeitet.

6 Klicken Sie auf **Weiter**.

Das Dialogfeld **Netzwerkzugang** wird angezeigt.



Virtuelle Maschinen greifen über Uplink-Adapter auf physische Netzwerke zu. Ein vSwitch kann nur dann Daten in externe Netzwerke übertragen, wenn mindestens ein Netzwerkadapter an den vSwitch angeschlossen ist. Wenn zwei oder mehr Adapter an einen vSwitch angeschlossen sind, werden sie transparent geteamt.

7 Klicken Sie auf **Virtuellen Switch erstellen**.

Sie können einen neuen vSwitch mit oder ohne Ethernet-Adapter erstellen.

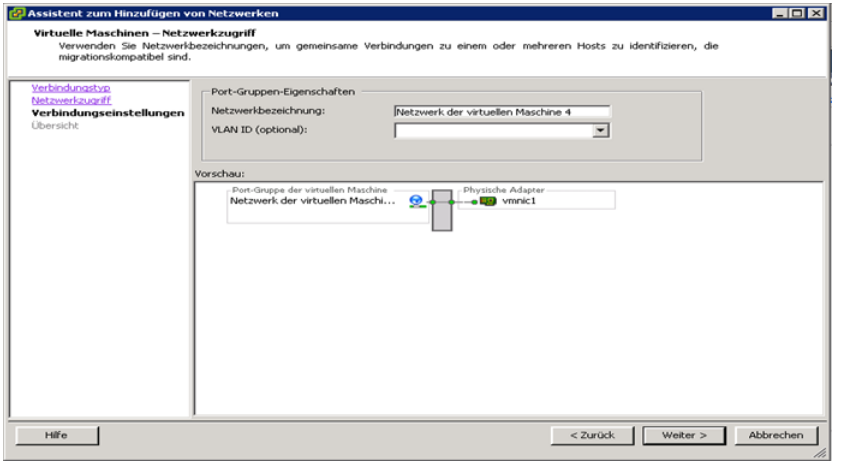
Wenn Sie einen vSwitch ohne physische Netzwerkadapter erstellen, ist der Datenverkehr auf diesem vSwitch auf diesen vSwitch beschränkt. Andere Hosts in dem physischen Netzwerk oder in virtuellen Maschinen auf anderen vSwitches können dann keine Daten über diesen vSwitch versenden oder empfangen. Das kann wünschenswert sein, wenn eine Gruppe von virtuellen Maschinen untereinander kommunizieren soll, nicht jedoch mit anderen Hosts oder virtuellen Maschinen außerhalb der Gruppe.

Die Auswahlmöglichkeiten werden im Bereich **Vorschau** angezeigt.

8 Klicken Sie auf **Weiter**.

Das Dialogfeld **Verbindungseinstellungen** wird angezeigt.

9 Geben Sie unter **Eigenschaften der Port-Gruppe** eine Netzwerkbezeichnung für die zu erstellende Port-Gruppe ein.



Mit den Netzwerkbezeichnungen können Sie migrationsfähige Verbindungen für zwei oder mehr Hosts identifizieren.

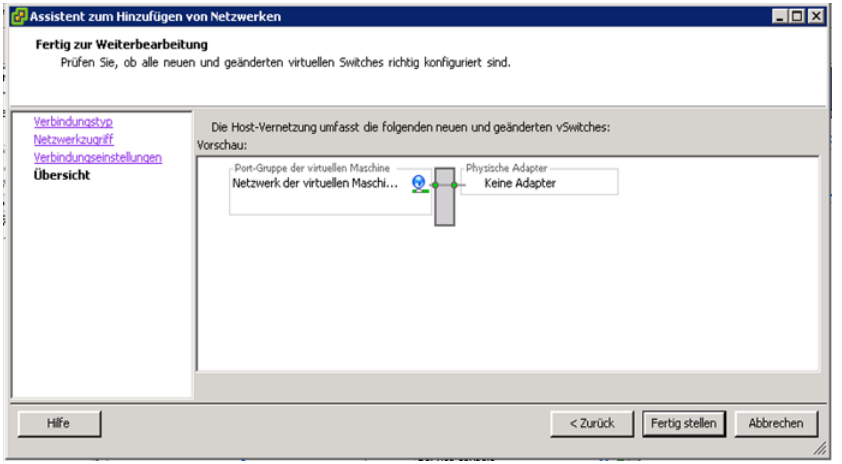
10 Wenn Sie ein VLAN verwenden, geben Sie im Feld **VLAN-ID** eine Zahl zwischen 1 und 4094 ein.

Wenn Sie sich nicht sicher sind, was hier eingegeben werden muss, lassen Sie das Feld frei oder wenden Sie sich an Ihren Netzwerkadministrator.

Wenn Sie 0 eingeben oder das Feld leer lassen, kann die Port-Gruppe nur ungetaggten (nicht-VLAN) Datenverkehr sehen. Wenn Sie 4095 eingeben, kann die Port-Gruppe jeden Datenverkehr auf einem VLAN sehen, und die VLAN-Tags bleiben intakt.

11 Klicken Sie auf **Weiter**.

Das Dialogfeld **Fertig stellen** wird angezeigt.



12 Überprüfen Sie die Konfiguration des vSwitches noch einmal und klicken Sie dann auf **Fertig stellen**.

HINWEIS Verbinden Sie mindestens zwei Adapter mit einem Switch, um Failover (NIC-Teaming) zu aktivieren. Wenn ein Uplink-Adapter versagt, wird der Datenverkehr des Netzwerkes auf einen anderen Adapter, der an den Switch angeschlossen ist, umgeleitet. NIC-Teambildung erfordert, dass beide Ethernet-Geräte auf demselben Ethernet-Übertragungsgebiet liegen.

Konfiguration des VMkernels

Die Verschiebung einer virtuellen Maschine von einem Host auf einen anderen wird Migration genannt. Die Migration einer aktivierten virtuellen Maschine nennt man VMotion. Die Migration mit VMotion, die zur Verwendung in hochkompatiblen Systemen entwickelt wurde, ermöglicht es Ihnen, virtuelle Maschinen ohne Ausfallzeiten zu verschieben. Der Protokollstapel des VMkernel muss richtig eingerichtet sein, damit VMotion ordnungsgemäß funktioniert.

„IP-Speicher“ bezeichnet jede Art von Speicher, die auf TCP/IP-Netzwerkkommunikation beruht. Dazu gehören iSCSI und NAS für ESX Server. Da diese beiden Speichertypen netzwerkbasiert sind, können beide die gleiche Port-Gruppe verwenden.

Die von VMkernel zur Verfügung gestellten Netzwerkdienste (iSCSI, NFS und VMotion) verwenden einen TCP/IP-Stapel im VMkernel. Dieser TCP/IP-Stapel ist vollständig getrennt von dem TCP/IP-Stapel, der in der Servicekonsole verwendet wird. Jeder dieser TCP/IP-Stapel greift durch die Anbindung mindestens eines vSwitches an mindestens eine Port-Gruppe auf verschiedene Netzwerke zu.

TCP/IP-Stapel auf Ebene der Überwachung der virtuellen

Der TCP/IP-Protokollstapel von VMware VMkernel wurde erweitert und kann jetzt iSCSI, NFS und VMotion folgendermaßen verarbeiten:

- iSCSI als Datastore für virtuelle Maschinen.
- iSCSI zur direkten Einbindung von .ISO Dateien, die von den virtuellen Maschinen als CD-ROMs erkannt werden.
- NFS als Datastore für virtuelle Maschinen.
- NFS zur direkten Einbindung von `.ISO` Dateien, die von den virtuellen Maschinen als CD-ROMs erkannt werden.
- Migration mit VMotion.

HINWEIS ESX unterstützt über TCP/IP nur NFS Version 3.

Schlussfolgerungen und Richtlinien

Beachten Sie sich bei der Konfiguration des VMkernel-Netzwerks folgende Richtlinien:

- Die IP-Adresse, die Sie der Servicekonsole während der Installation zuweisen, darf nicht der IP-Adresse entsprechen, die Sie dem TCP/IP-Stapel des VMkernel in der Registerkarte „Konfiguration > Netzwerk“ auf dem VI Client zugewiesen haben.
- Vor der Konfiguration des Software-iSCSI für den ESX Server-Host muss ein Firewall-Port durch Aktivierung des iSCSI-Software-Client-Dienstes geöffnet werden. Weitere Informationen finden Sie unter „Freigeben von Firewall-Ports für unterstützte Dienste und Management-Agenten“ auf Seite 192.
- Im Gegensatz zu anderen VMkernel-Diensten verfügt iSCSI über eine Servicekonsolenkomponente, sodass sowohl die Servicekonsole als auch VMkernel-TCP-IP-Stapel auf Netzwerke zugreifen können müssen, die zum Zugriff auf iSCSI-Ziele verwendet werden.

Einrichtung von VMkernel

1. Melden Sie sich am VMware VI Client an und wählen Sie den Server aus dem Inventar aus.

   Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

2. Klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Netzwerk**.
3. Klicken Sie auf den Link **Netzwerk hinzufügen**.

   Der **Assistent zum Hinzufügen von Netzwerken** wird angezeigt.

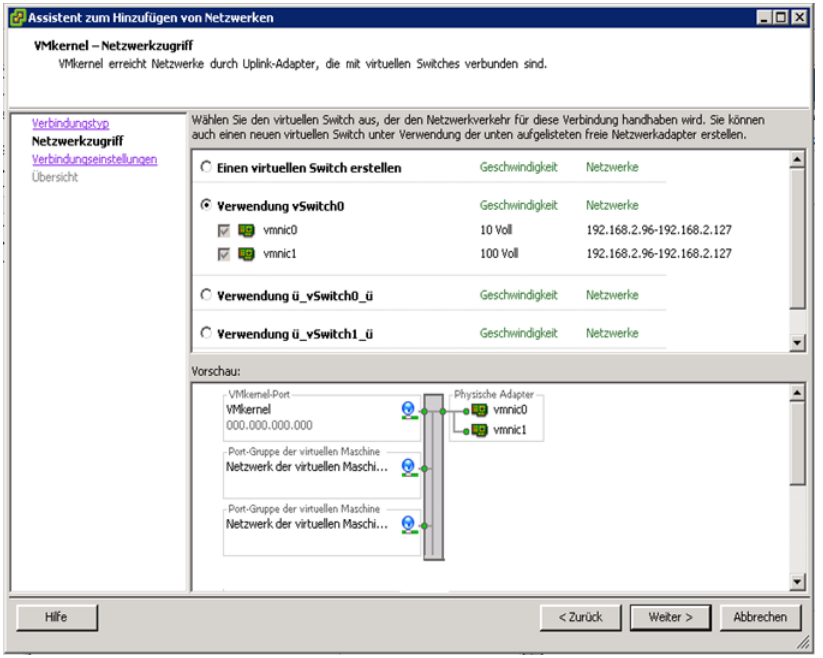
4. Wählen Sie **VMkernel** und klicken Sie auf **Weiter**.

Durch Auswahl der Option **VMotion und IP-Speicher** können Sie das VMkernel, das Dienste für VMotion und IP-Speicher (NFS oder iSCSI) ausführt, an ein physisches Netzwerk anschließen.

Das Dialogfeld **Netzwerkzugang** wird angezeigt.

5 Wählen Sie den vSwitch aus, den Sie verwenden möchten, oder aktivieren Sie das Optionsfeld **Einen virtuellen Switch erstellen,** um einen neuen vSwitch anzulegen.

6 Aktivieren Sie die Kontrollkästchen für die Netzwerkadapter, die Ihr vSwitch verwenden soll.



Die Auswahlmöglichkeiten werden im Bereich **Vorschau** angezeigt.

Wählen Sie für jeden vSwitch Adapter aus, sodass die virtuellen Maschinen, die an diesen Adapter angeschlossen sind, auf das richtige Ethernet-Segment zugreifen können. Wenn unter **Neuen virtuellen Switch erstellen** keine Adapter angezeigt werden, bedeutet dies, dass alle Netzwerkadapter im System von vorhandenen vSwitches verwendet werden. Sie können entweder einen neuen vSwitch ohne Netzwerkadapter erstellen oder einen Netzwerkadapter auswählen, der von einem bereits vorhandenen vSwitch verwendet wird.

Weiter Informationen zum Bewegen von Netzwerkadaptern zwischen vSwitches finden Sie unter „Hinzufügen von Uplink-Adaptern“ auf Seite 50.

7 Klicken Sie auf **Weiter**.

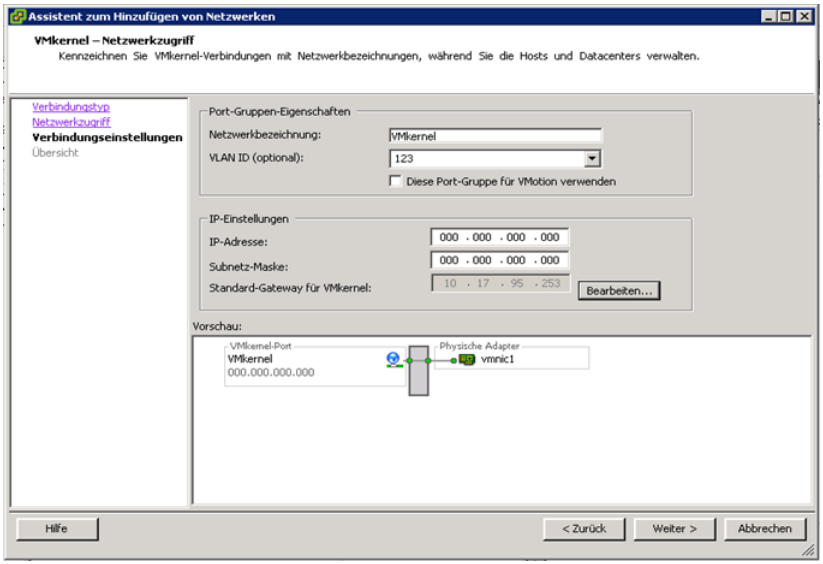
Das Dialogfeld **Verbindungseinstellungen** wird angezeigt.

8 Wählen Sie eine Netzwerkbezeichnung und eine VLAN-ID unter **Eigenschaften der Port-Gruppe** aus bzw. geben Sie diese ein.

- **Netzwerkbezeichnung** – Ein Name, der die Port-Gruppe bezeichnet, die erstellt wird. Es handelt sich dabei um die Bezeichnung, die Sie bei der Konfiguration von VMkernel-Diensten wie VMotion und IP-Speicher während der Konfiguration des virtuellen Adapters, der an diese Port-Gruppe angeschlossen wird, festlegen.
- **VLAN-ID** – Bezeichnet das VLAN, das für den Netzwerkdatenverkehr der Port-Gruppe verwendet wird.

9 Aktivieren Sie das Kontrollkästchen **Diese Port-Gruppe für VMotion verwenden**, damit diese Port-Gruppe anderen ESX Servern melden kann, dass sie die Netzwerkverbindung ist, an die VMotion-Datenverkehr gesendet werden soll.

Auf jedem ESX Server-Host kann diese Eigenschaft nur für eine VMotion- und IP-Speicher-Port-Gruppe aktiviert werden. Wenn diese Eigenschaft für keine der Port-Gruppen aktiviert wurde, ist eine VMotion-Migration auf diesen Host nicht möglich.



10 Klicken Sie unter **IP-Einstellungen** auf **Bearbeiten** um die **Standard-Gateway für VMkernel** für VMkernel-Dienste wie z. B. VMotion, NAS und iSCSI einzurichten.

HINWEIS Die Standard-Gateway für den Port, den Sie erstellen, muss eingestellt werden. VirtualCenter 2 unterscheidet sich hier von VirtualCenter 1.x. Sie müssen zur Konfiguration des VMkernel-IP-Stapels eine gültige IP-Adresse verwenden, keine Pseudoadresse.

Das Dialogfeld **DNS und Routing-Konfiguration** wird angezeigt. Auf der Registerkarte **DNS-Konfiguration** ist im Namensfeld standardmäßig der Hostname eingetragen. Auch die DNS-Server-Adressen und die Domäne, die während der Installation angegeben wurden, werden automatisch ausgefüllt.

Auf der Registerkarte **Routing** benötigen die Servicekonsole und das VMkernel jeweils eigene Gateway-Angaben. Eine Gateway ist zur Anbindung an Computer notwendig, die sich nicht im gleichen IP-Subnetz wie die Servicekonsole oder das VMkernel befinden.

Standardmäßig ist „Statische IP“ eingestellt.

11 Klicken Sie auf **OK**, um die Änderungen zu speichern und das Dialogfeld **DNS-Konfiguration und Routing** zu schließen.

12 Klicken Sie auf **Weiter**.

13 Wenn Sie Änderungen vornehmen möchten, verwenden Sie die Schaltfläche **Zurück**.

14 Überprüfen Sie die Änderungen im Dialogfeld **Fertig stellen** und klicken Sie auf **Fertig stellen**.

Konfiguration der Servicekonsole

Sowohl die Servicekonsole als auch das VMkernel verwenden virtuelle Ethernet-Adapter zur Anbindung an einen vSwitch und zum Zugriff auf Netzwerke über diesen vSwitch.

Grundlegende Konfigurationsaufgaben für die Servicekonsole

Es gibt zwei häufig auftretende Konfigurationsänderungen für die Servicekonsole: Die Änderung von Netzwerkkarten (NICs) und die Änderung von Einstellungen für eine bestehende, sich in Verwendung befindende Netzwerkkarte.

Eine Änderung der Servicekonsolenkonfiguration ist nicht zulässig, wenn nur ein Servicekonsolenanschluss vorhanden ist. Wenn Sie eine neue Verbindung herstellen möchten, müssen Sie die Netzwerkeinstellungen so ändern, dass eine weitere Netzwerkkarte verwendet wird. Nach der Überprüfung der Funktionsfähigkeit des neuen Anschlusses kann der alte Anschluss entfernt werden. Im Prinzip wird also die Netzwerkkarte gewechselt.

Konfiguration der Netzwerk-Servicekonsole

1 Melden Sie sich am VMware VI Client an und wählen Sie den Server aus dem Inventar aus.

Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

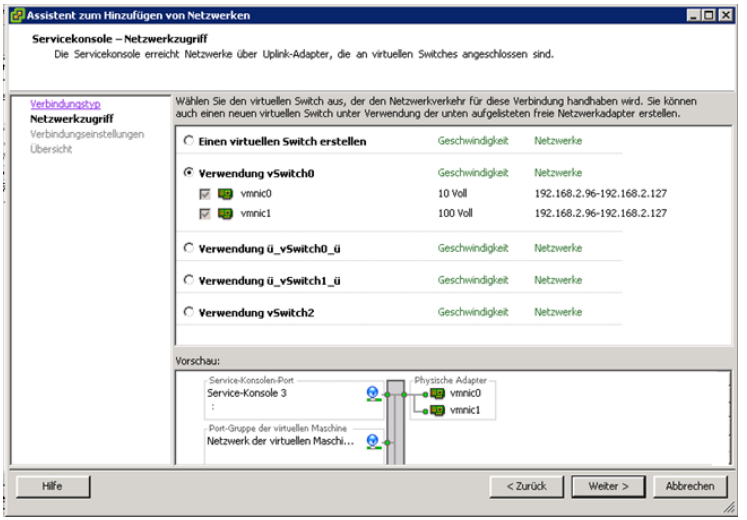
2 Klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Netzwerk**.

3 Klicken Sie auf den Link **Netzwerk hinzufügen**.

Der **Assistent zum Hinzufügen von Netzwerken** wird angezeigt.

4 Wählen Sie im Dialogfeld **Verbindungsarten** die Option **Servicekonsole** und klicken Sie auf **Weiter**.

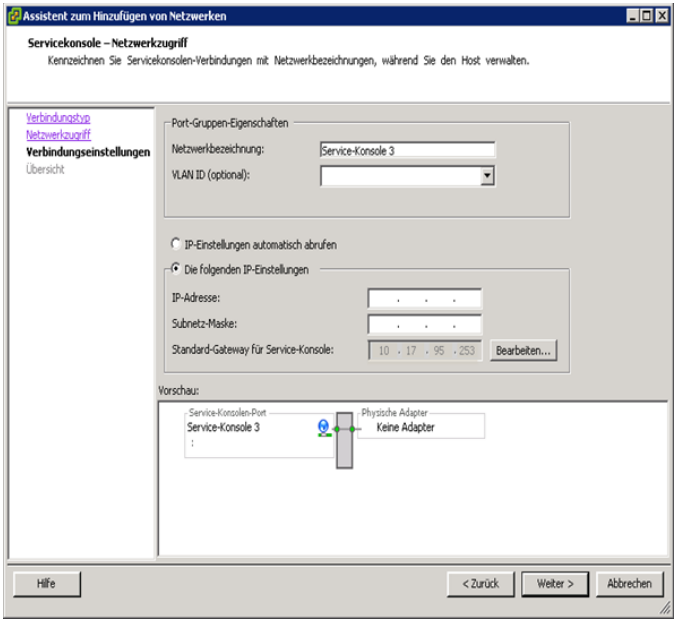
Das Dialogfeld **Netzwerkzugriff der Servicekonsole** wird angezeigt.



5 Wählen Sie den vSwitch aus, den Sie für den Zugriff auf das Netzwerk verwenden möchten, oder markieren Sie **Neuen vSwitch erstellen**. Klicken Sie auf **Weiter**.

Wenn unter **Neuen virtuellen Switch erstellen** keine Adapter angezeigt werden, bedeutet dies, dass alle Netzwerkadapter im System von vorhandenen vSwitches verwendet werden. Weiter Informationen zum Bewegen von Netzwerkadaptern zwischen vSwitches finden Sie unter „Hinzufügen von Uplink-Adaptern“ auf Seite 50.

6 Unter **Port-Gruppen-Eigenschaften** wählen Sie **Netzwerkbezeichnung** und **VLAN-ID** aus bzw. geben Sie diese ein.



Neuere Ports und Port-Gruppen werden im vSwitch-Diagramm oben angezeigt.

7 Geben Sie die **IP-Adresse** und die **Subnetzmaske** ein oder aktivieren Sie die DHCP-Option **IP-Einstellung automatisch beziehen** für die IP-Adresse und die Subnetzmaske.

8 Klicken Sie auf die Schaltfläche **Bearbeiten**, um die **Standard-Gateway der Servicekonsole** einzustellen.

Weitere Informationen finden Sie unter „Einstellung der Standard-Gateway“ auf Seite 41.

9 Klicken Sie auf **Weiter**.

Das Dialogfeld **Fertig stellen** wird angezeigt.

10 Überprüfen Sie die Angaben und klicken Sie auf **Fertig stellen**.

Konfiguration der Servicekonsolen-Ports

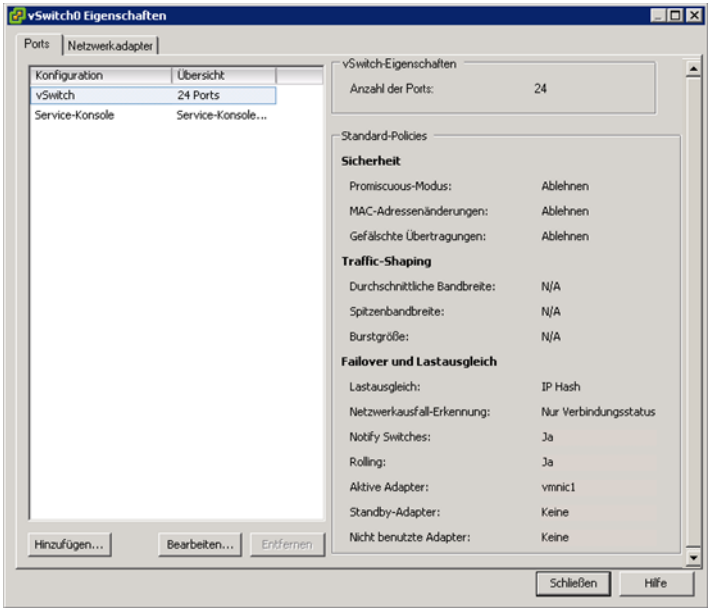
1 Melden Sie sich am VMware VI Client an und wählen Sie den Server aus dem Inventar aus.

Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Netzwerk**.

3 Suchen Sie auf der rechten Bildschirmseite den vSwitch, den Sie bearbeiten möchten, und klicken Sie für diesen vSwitch auf **Eigenschaften**.

Das Dialogfeld **vSwitch Properties** (vSwitch-Eigenschaften) wird angezeigt.



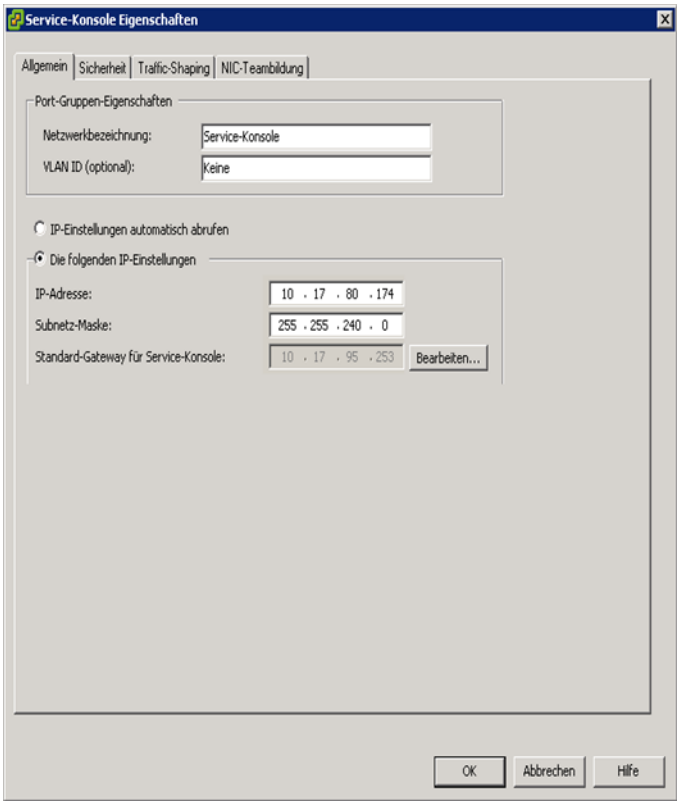
4 Klicken Sie im Dialogfeld **vSwitch Properties** (vSwitch-Eigenschaften) auf die Registerkarte **Ports**.

5 Markieren Sie die Option **Servicekonsole** und klicken Sie auf **Bearbeiten**.

Es wird eine Warnmeldung angezeigt, dass die Änderung des Servicekonsolen-anschlusses die Verbindungen für alle Management-Agenten trennen kann.

6 Klicken Sie auf **Änderung dieser Verbindung fortsetzen**, um mit der Konfiguration der Servicekonsole fortzufahren.

Das Dialogfeld **Port-Eigenschaften der Servicekonsole** wird angezeigt.



7 Bearbeiten Sie die Port-Eigenschaften, die IP-Einstellungen und die verwendeten Policys entsprechend.

8 Klicken Sie auf OK.

Pro TCP/IP-Stapel kann nur eine Standard-Gateway verwendet werden.

Einstellung der Standard-Gateway

1 Melden Sie sich am VMware VI Client an und wählen Sie den Server aus dem Inventar aus.

Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration** und dort auf **DNS und Routing**.

Das Dialogfeld **DNS und Routing** wird angezeigt.

3 Klicken Sie auf **Eigenschaften**.

Das Dialogfeld **DNS-Konfiguration** wird angezeigt.

Auf der Registerkarte **DNS-Konfiguration** ist im Namensfeld standardmäßig der Hostname eingetragen. Auch die DNS-Server-Adressen und die Domäne, die während der Installation angegeben wurden, werden automatisch eingetragen.

Auf der Registerkarte **Routing** sind die Servicekonsole und das VMkernel oft nicht an das gleiche Netzwerk angeschlossen und benötigen daher jeweils eigene Gateway-Daten. Eine Gateway ist zur Anbindung an Computer notwendig, die sich nicht im gleichen IP-Subnetz wie die Servicekonsole oder das VMkernel befinden.

HINWEIS Alle NAS- und iSCSI-Server müssen entweder über den Standard-Gateway oder über dasselbe Übertragungsgebiet wie die zugeordneten vSwitches zu erreichen sein.

Bei der Servicekonsole ist eine Gateway nur notwendig, wenn mindestens zwei Netzwerkadapter das gleiche Subnetz verwenden. Die Gateway bestimmt, welcher Netzwerk-Adapter für die Standardroute verwendet wird.

4 Klicken Sie auf die Registerkarte **Routing**.

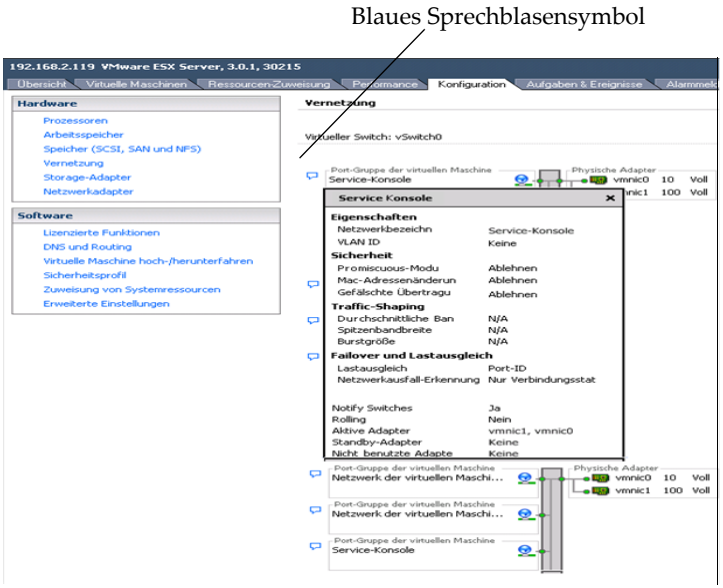
5 Stellen Sie die Standard-Gateway des VMkernels ein.

VORSICHT Es besteht das Risiko der Fehlkonfiguration, wodurch die Anwenderschnittstelle die Anbindung an den Host verlieren kann. In diesem Fall muss der Host über die Befehlszeileneingabe der Servicekonsole neu konfiguriert werden.

6 Klicken Sie auf **OK**, um die Änderungen zu speichern und das Dialogfeld **DNS-Konfiguration** zu schließen.

Anzeige von Servicekonsoleninformationen

1 Klicken Sie zur Anzeige von Servicekonsoleninformationen auf das blaue Sprechblasensymbol.



2 Wenn Sie das Popup-Fenster schließen möchten, klicken Sie auf **X**.

Verwendung von DHCP für die Servicekonsole

In den meisten Fällen sollten für die Servicekonsole statische IP-Adressen verwendet werden. Wenn Ihr DNS-Server in der Lage ist, der dynamisch generierten IP-Adresse den Hostnamen der Servicekonsole zuzuordnen, können Sie für die Servicekonsole auch die dynamische IP-Adressierung (DHCP) verwenden.

Wenn der DNS-Server den Hostnamen nicht zur dynamischen IP-Adresse zuweisen kann, müssen Sie die numerische IP-Adresse der Servicekonsole bestimmen und diese numerische IP-Adresse verwenden, wenn Sie auf die Webseiten der Schnittstelle zugreifen.

Diese numerische IP-Adresse kann sich ändern, wenn DHCP-Zuweisungen auslaufen oder wenn das System neu gestartet wird. Aus diesem Grund wird die Verwendung von DHCP für die Servicekonsole nicht empfohlen, wenn der DNS-Server die Hostnamen-Übersetzung nicht durchführen kann.

Erweiterte Netzwerkeigenschaften 3

Dieses Kapitel führt Sie durch die erweiterten Netzwerkfragen in einer ESX Server-Umgebung und durch die Einrichtung und Änderung der erweiterten Netzwerkkonfigurationsoptionen.

In diesem Kapitel werden folgende Themen behandelt:

- „Erweiterte Netzwerkaufgaben“ auf Seite 46
- „Konfiguration des virtueller Switch“ auf Seite 46
- „Konfigurieren der Port-Gruppe“ auf Seite 60
- „DNS und Routing“ auf Seite 62
- „Einrichten von MAC-Adressen“ auf Seite 64
- „Netzwerk-Tipps und Empfehlungen“ auf Seite 67

Erweiterte Netzwerkaufgaben

Dieses Kapitel erklärt, wie die folgenden erweiterten Netzwerkaufgaben ausgeführt werden:

- „Bearbeitung der Port-Anzahl für einen vSwitch“ auf Seite 46
- „Konfiguration der Geschwindigkeit des Uplink-Netzwerkadapters“ auf Seite 49
- „Hinzufügen von Uplink-Adaptern“ auf Seite 50
- „Bearbeiten der Sicherheits-Policy für Layer 2:“ auf Seite 53
- „Bearbeiten der Traffic-Shaping-Policy“ auf Seite 55
- „Bearbeiten der Policy für Failover und Lastausgleich“ auf Seite 57
- „Bearbeiten der Eigenschaften von Port-Gruppen“ auf Seite 60
- „So setzen Sie die Policys für bezeichnete Netzwerke außer Kraft“ auf Seite 61
- „Ändern der DNS- und Routing-Konfiguration“ auf Seite 62
- „So richten Sie eine MAC-Adresse ein“ auf Seite 66

Konfiguration des virtueller Switch

In diesem Abschnitt werden folgende Themen behandelt:

- „Eigenschaften von virtuellen Switches“ auf Seite 46
- „Policys für virtuelle Switches“ auf Seite 53

Eigenschaften von virtuellen Switches

Die vSwitch-Einstellungen steuern Port-Standardeinstellungen für den ganzen vSwitch; diese Port-Einstellungen können durch Port-Gruppeneinstellungen außer Kraft gesetzt werden.

Bearbeiten der Eigenschaften von virtuellen Switches

Zur Bearbeitung der vSwitch-Eigenschaften gehört:

- die Konfiguration von Ports
- die Konfiguration des Uplink-Netzwerkadapters

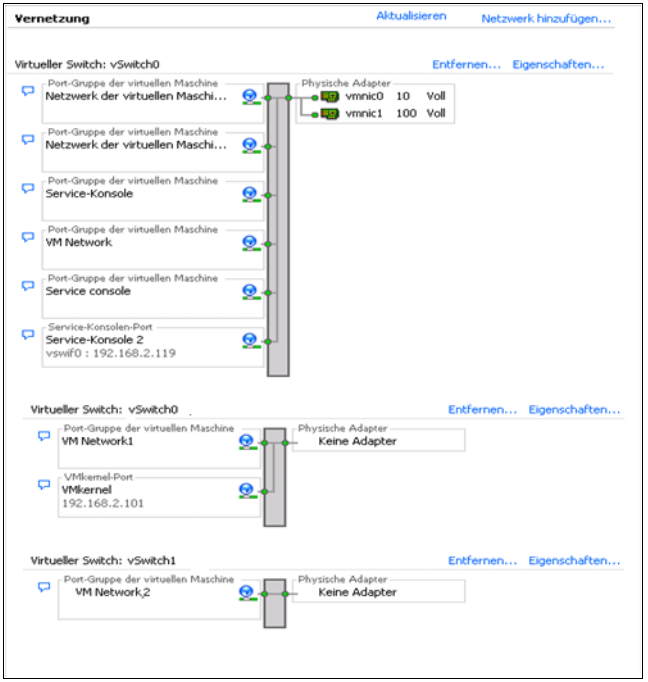
Bearbeitung der Port-Anzahl für einen vSwitch

1. Melden Sie sich am VMware VI Client an und wählen Sie den Server aus dem Inventar aus.

   Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

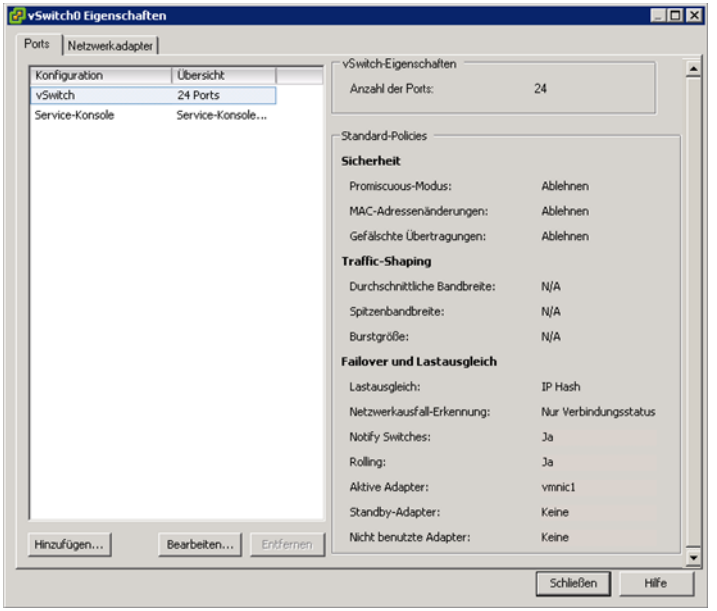
2. Klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Netzwerk**.

3 Suchen Sie auf der rechten Bildschirmseite den vSwitch, den Sie bearbeiten möchten.



4 Klicken Sie auf **Eigenschaften** für diesen vSwitch.

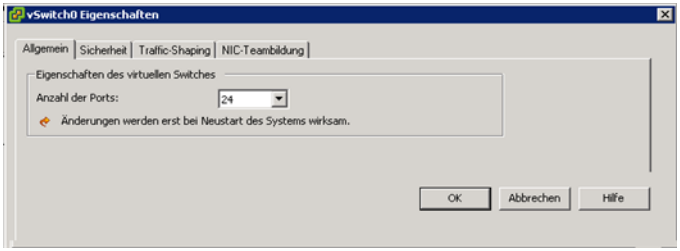
Das Dialogfeld **vSwitch-Eigenschaften** wird angezeigt.



5 Klicken Sie auf die Registerkarte **Ports**.

6 Markieren Sie den vSwitch in der Liste **Konfiguration** und klicken Sie auf **Bearbeiten**.

Das Dialogfeld **vSwitch-Eigenschaften** wird angezeigt.



7 Klicken Sie auf die Registerkarte **Allgemein**, um die Port-Anzahl festzulegen.

8 Wählen Sie die Anzahl der Ports, die Sie verwenden möchten, oder geben Sie sie ein.

Änderungen treten erst in Kraft, wenn Sie ESX Server neu starten.

9 Klicken Sie auf **OK**.

Konfiguration der Geschwindigkeit des Uplink-Netzwerkadapters

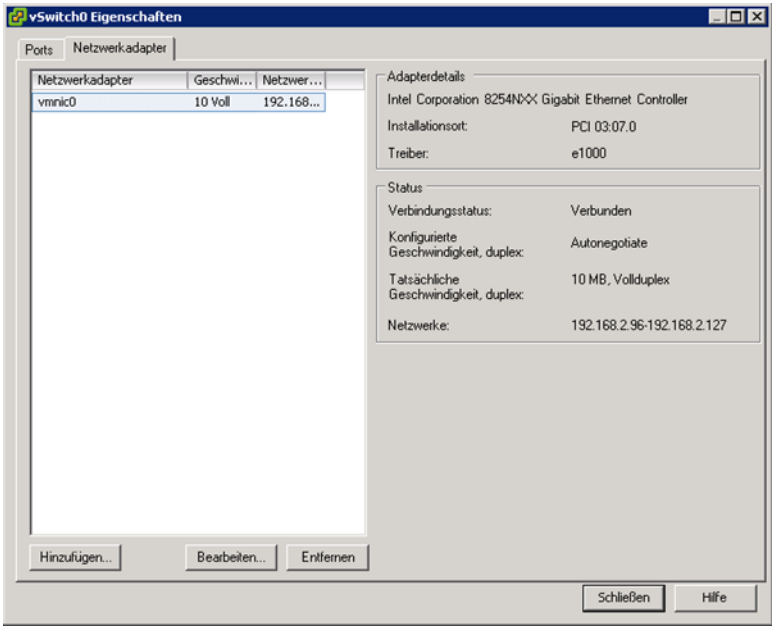
1 Melden Sie sich am VMware VI Client an und wählen Sie den Server aus dem Inventar aus.

Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Netzwerk**.

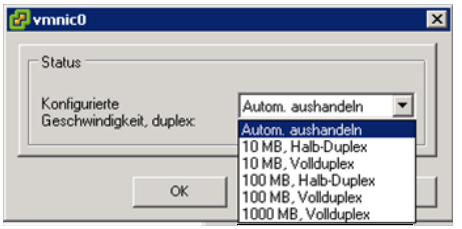
3 Markieren Sie einen vSwitch und klicken Sie auf **Eigenschaften**.

4 Klicken Sie im Dialogfeld **vSwitch-Eigenschaften** auf die Registerkarte **Netzwerkadapter**.



5 Um die eingestellte Geschwindigkeit (den Duplexwert) eines Netzwerkadapters zu ändern, markieren Sie den Netzwerkadapter und klicken Sie auf **Bearbeiten**.

Das Dialogfeld **Status** wird angezeigt. Die Standardeinstellung lautet **Autonegotiate**, die meistens richtig ist.



6 Um die Verbindungsgeschwindigkeit manuell einzustellen, wählen Sie die Geschwindigkeit/Duplexeinstellung aus dem Drop-Down-Menü aus.

Die Verbindungsgeschwindigkeit muss manuell eingestellt werden, wenn die Netzwerkkarte oder ein physischer Switch die richtige Verbindungsgeschwindigkeit nicht erkennen. Anzeichen für falsch eingestellte Geschwindigkeit/Duplex sind niedrige Bandbreite oder völlig fehlende Konnektivität.

Der Adapter und der physische Switch-Port, an den der Adapter angeschlossen ist, müssen auf den gleichen Wert gesetzt werden, entweder Auto/Auto oder ND/ND (wobei ND für die Geschwindigkeit/Duplex steht), nicht jedoch Auto/ND.

7 Klicken Sie auf **OK**.

Hinzufügen von Uplink-Adaptern

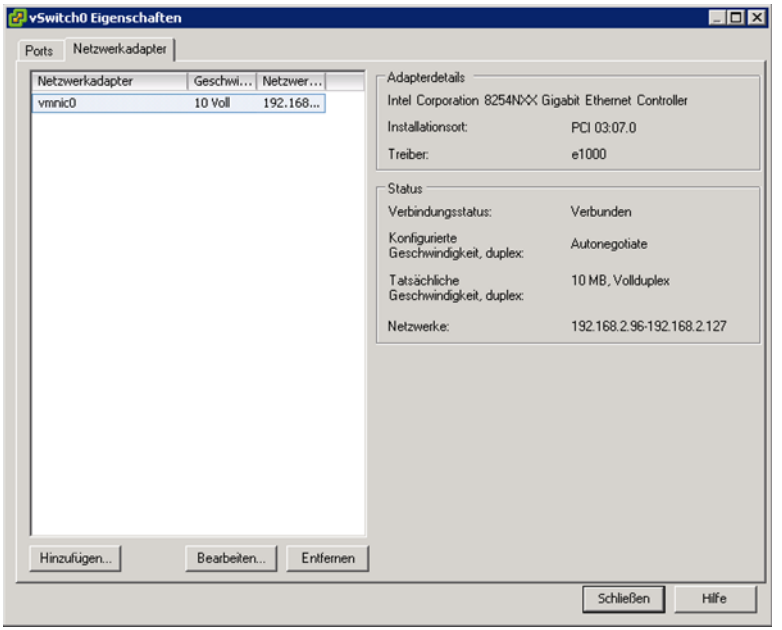
1 Melden Sie sich am VMware VI Client an und wählen Sie den Server aus dem Inventar aus.

Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Netzwerk**.

3 Markieren Sie einen vSwitch und klicken Sie auf **Eigenschaften**.

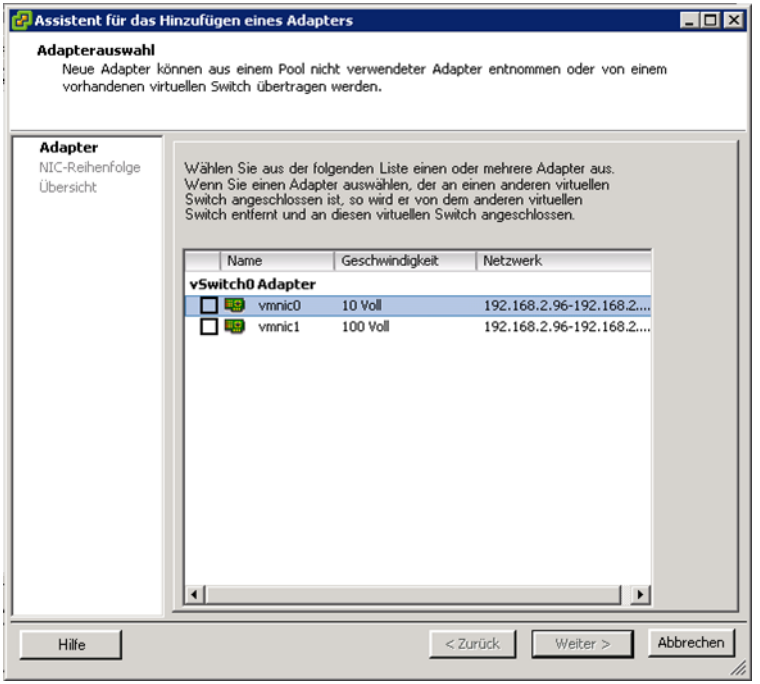
4 Klicken Sie im Dialogfeld **vSwitch-Eigenschaften** auf die Registerkarte **Netzwerkadapter**.



5 Klicken Sie auf **Hinzufügen**. Der Assistent zum Hinzufügen eines Adapters wird aufgerufen.

Sie können einem einzelnen vSwitch mehrere Adapter zuweisen, um NIC-Teaming zu erzielen. Eine solches Team kann den Datenverkehr unter sich aufteilen und Ausfallsicherheit gewährleisten.

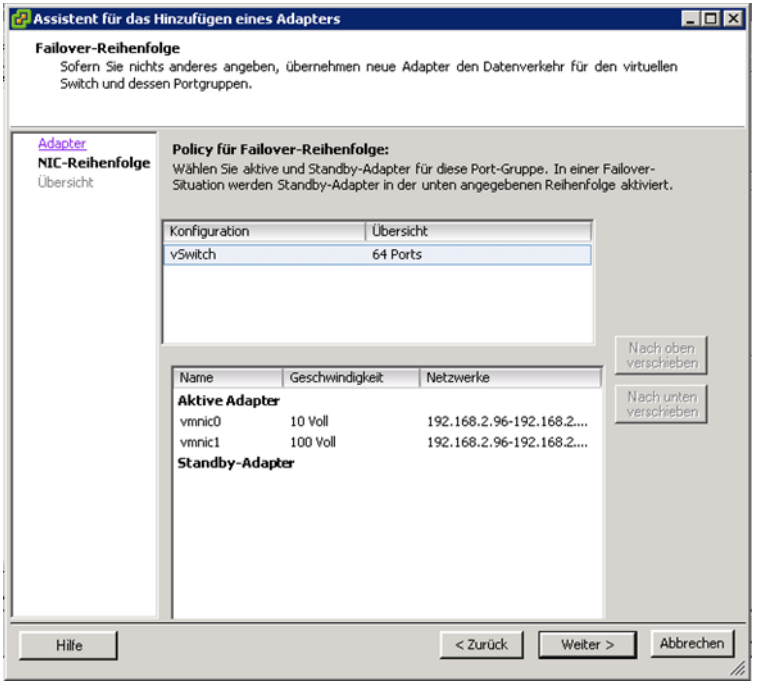
VORSICHT Eine Fehlkonfiguration kann dazu führen, dass der VI Client nicht mehr auf den Host zugreifen kann.


Assistent für das Hinzufügen eines Adapters
Adapterauswahl
Neue Adapter können aus einem Pool nicht verwendeter Adapter entnommen oder von einem vorhandenen virtuellen Switch übertragen werden.
Adapter
NIC-Reihenfolge
Übersicht
Wählen Sie aus der folgenden Liste einen oder mehrere Adapter aus. Wenn Sie einen Adapter auswählen, der an einen anderen virtuellen Switch angeschlossen ist, so wird er von dem anderen virtuellen Switch entfernt und an diesen virtuellen Switch angeschlossen.
Name
Geschwindigkeit
Netzwerk
vSwitch0 Adapter
vmnic0
10 Voll
192.168.2.96-192.168.2....
vmnic1
100 Voll
192.168.2.96-192.168.2....
Hilfe
< Zurück
Weiter >
Abbrechen

6 Wählen Sie mindestens einen Adapter aus der Liste aus und klicken Sie auf **Weiter**.

7 Sie können die Netzwerkkarten ordnen, indem Sie eine dieser Karten auswählen und auf die entsprechenden Schaltflächen klicken, um die Karte nach oben oder unten oder in eine andere Kategorie (Aktiv oder Standby) zu verschieben.

- **Aktive Adapter** – Adapter, die derzeit durch den vSwitch verwendet werden.
- **Standby-Adapter** – Adapter, die dann aktiviert werden, wenn einer oder mehrere der aktiven Adapter ausfallen.



8 Klicken Sie auf **Weiter**.

Das Dialogfeld **Adapterübersicht** wird angezeigt.

9 Überprüfen Sie die Angaben in diesem Dialogfeld. Verwenden Sie die Schaltfläche **Zurück**, um Änderungen vorzunehmen, oder klicken Sie auf **Fertig stellen**, um den Assistenten zum Hinzufügen eines Adapters zu beenden.

Die Liste der Netzwerkadapter mit den nun dem vSwitch zugewiesenen Adaptern wird erneut angezeigt.

10 Klicken Sie auf **Schließen**, um das Dialogfeld **vSwitch-Eigenschaften** zu verlassen.

Der Abschnitt **Netzwerk** auf der Registerkarte **Konfiguration** zeigt die Netzwerkadapter in ihrer festgelegten Reihenfolge und den gewählten Kategorien.

Policys für virtuelle Switches

Sie können Policys für den ganzen vSwitch festlegen, indem Sie den vSwitch oben auf der Registerkarte **Ports** auswählen und auf **Bearbeiten** klicken.

Wenn Sie eine dieser Einstellungen für eine bestimmte Port-Gruppe ändern möchten, markieren Sie diese Port-Gruppe und klicken Sie auf **Bearbeiten**. Alle Änderungen der Einstellungen für den ganzen vSwitch werden auf alle Port-Gruppen des vSwitches angewendet, ausgenommen hiervon sind die Konfigurationsoptionen, die für die Port-Gruppe festgelegt wurden.

Es gibt folgende Policys für vSwitches:

- Sicherheits-Policy für Layer 2
- Traffic-Shaping-Policy
- Policy für Lastausgleich und Failover

Sicherheits-Policy für Layer 2

Layer 2 (L2) ist die Daten-Link-Layer. Die drei Elemente der Sicherheits-Policy für Layer 2 sind der Promiscuous-Modus, Änderungen der MAC-Adresse und gefälschte Übertragungen.

Wenn der Promiscuous-Modus nicht aktiviert wurde, erkennt der Gastadapter nur Datenverkehr auf seiner eigenen MAC-Adresse. Im Promiscuous-Modus erkennt er alle Datenpakete. Standardmäßig ist Promiscuous-Modus für die Gastadapter deaktiviert.

Weitere Informationen zur Sicherheit finden Sie unter „Absicherung der Ports virtueller Switches“ auf Seite 201.

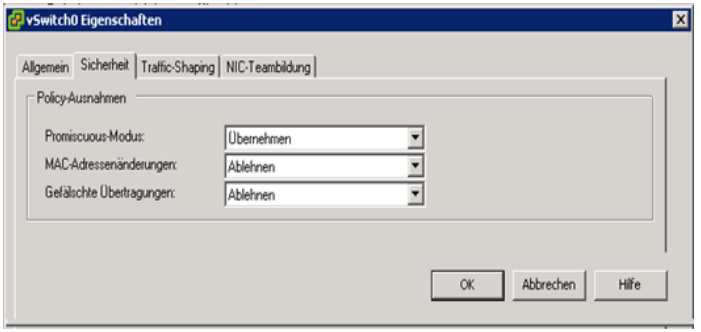
Bearbeiten der Sicherheits-Policy für Layer 2:

1. Melden Sie sich am VMware VI Client an und wählen Sie den Server aus dem Inventar aus.

   Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

2. Klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Netzwerk**.
3. Klicken Sie für den vSwitch, dessen L2-Sicherheits-Policy Sie bearbeiten möchten, auf **Eigenschaften**.
4. Klicken Sie im Dialogfeld **vSwitch-Eigenschaften** auf die Registerkarte **Ports**.
5. Markieren Sie „vSwitch“ und klicken Sie auf **Bearbeiten**.

6 Klicken Sie im Dialogfeld „vSwitch-Eigenschaften“ auf die Registerkarte **Sicherheit**.



In der Standardeinstellung ist die Option **Promiscuous-Modus** auf **Ablehnen** gesetzt und **Änderungen der MAC-Adresse** und **Forced Transmits** sind auf **Akzeptieren** gesetzt.

Diese Policy gilt für alle virtuellen Adapter auf dem vSwitch, außer für diejenigen, für die die Port-Gruppe für die virtuellen Adapter eine Ausnahme von der Policy beschreibt.

7 Im Bereich **Policy-Ausnahmen** können Sie auswählen, ob die Ausnahmen für die L2-Sicherheits-Policy abgelehnt oder angenommen werden sollen:

- **Promiscuous-Modus**
  - **Ablehnen** – Die Aktivierung des Promiscuous-Modus für den Gast-Adapter hat keine Auswirkungen darauf, welche Frames vom Adapter empfangen werden.
  - **Akzeptieren** – Die Aktivierung des Promiscuous-Modus für den Gast-Adapter veranlasst, dass alle Frames erkannt werden, die über den vSwitch übertragen werden und die nach der VLAN-Policy für die Port-Gruppe, an die der Adapter angeschlossen ist, zugelassen sind.
- **Änderungen der MAC-Adresse**
  - **Ablehnen** – Wenn die Option **Änderungen der MAC-Adresse** auf **Ablehnen** gesetzt ist, und das Gast-Betriebssystem ändert die MAC-Adresse auf einen anderen Wert als den, der in der Konfigurationsdatei `.vmx` angegeben ist, werden alle ankommenden Frames verworfen.

    Wenn das Gast-Betriebssystem die MAC-Adresse wieder auf eine MAC-Adresse ändert, die in der `.vmx` Konfigurationsdatei angegeben ist, werden alle ankommenden Datenblöcke wieder weitergeleitet.

- **Akzeptieren** – Die Änderung der MAC-Adresse des Gast-Betriebssystems hat den gewünschten Effekt: Datenblöcke an die neue MAC-Adresse werden empfangen.

- **Gefälschte Übertragungen**
  - **Ablehnen** – Alle ausgehenden Datenblöcke, bei denen die Quell-MAC-Adresse sich von der auf dem Adapter eingestellten MAC-Adresse unterscheidet, werden verworfen.
  - **Akzeptieren** – Eine wird keine Filterung vorgenommen und alle ausgehenden Frames werden weitergeleitet.

8 Klicken Sie auf **OK**.

Traffic-Shaping-Policy

ESX Server passt den Datenverkehr durch die Aufstellung von Parametern für drei ausgehende Datenverkehrsmerkmale an: durchschnittliche Bandbreite, Burstgröße und Spitzenbandbreite. Sie können die Werte für diese Merkmale über den VI Client einstellen und somit die Traffic-Shaping-Policy für jeden Uplink-Adapter festlegen.

- Die **Durchschnittliche Bandbreite** legt die Anzahl der Bits pro Sekunde fest, die–die zulässige durchschnittliche Datenlast durchschnittlich im Zeitverlauf über den vSwitch passieren darf.
- **Burstgröße** legt die Höchstanzahl der Bytes fest, die in einem Burst zulässig sind. Wenn ein Burst diesen Wert überschreitet, werden überschüssige Datenpakete für die spätere Übertragung in die Warteschlange eingereiht. Wenn die Warteschlange voll ist, werden die Pakete verworfen. Wenn Sie Werte für diese beiden Merkmale festlegen, zeigen Sie an, was der vSwitch während des Normalbetriebs verarbeiten soll.
- Die **Spitzenbandbreite** ist die höchste Bandbreite, die der vSwitch bereitstellen kann, ohne Pakete verwerfen zu müssen. Wenn der Datenverkehr die festgelegte Spitzenbandbreite übersteigt, werden überschüssige Pakete für die spätere Übertragung (wenn der Datenverkehr wieder auf ein normales Maß zurückgegangen ist und genügend Reservezyklen zur Verarbeitung der Pakete zur Verfügung stehen) in die Warteschlange eingereiht. Wenn die Warteschlange voll ist, werden die Pakete verworfen. Selbst wenn Sie über Reservebandbreite verfügen, weil die Verbindung sich im Leerlauf befindet, beschränkt der Parameter „Spitzenbandbreite“ die Übertragung auf den festgelegten Spitzenwert, bis der Datenverkehr zur zulässigen Durchschnittsdatenlast zurückkehrt.

Bearbeiten der Traffic-Shaping-Policy

1 Melden Sie sich am VMware VI Client an und wählen Sie den Server aus dem Inventar aus.

  Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Netzwerk**.

3 Markieren Sie einen vSwitch und klicken Sie auf **Eigenschaften**.

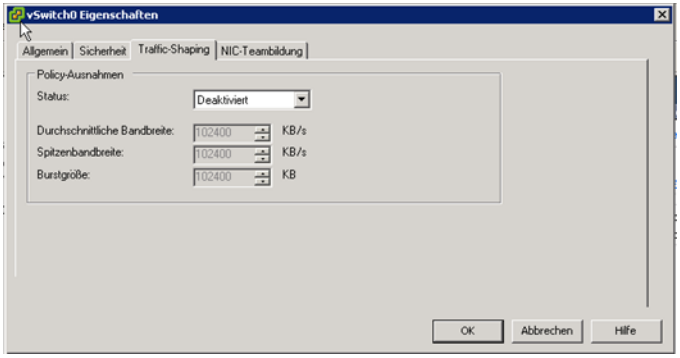
4 Klicken Sie im Dialogfeld **vSwitch-Eigenschaften** auf die Registerkarte **Ports**.

5 Markieren Sie den vSwitch und klicken Sie auf **Bearbeiten**.

Das Dialogfeld **Eigenschaften** für den ausgewählten vSwitch wird angezeigt.

6 Klicken Sie auf die Registerkarte **Traffic-Shaping**.

Das Dialogfeld **Policy-Ausnahmen** wird angezeigt. Wenn Traffic-Shaping deaktiviert ist, sind die einstellbaren Funktionen grau unterlegt. Sie können alle Traffic-Shaping-Funktionen selektiv auf Port-Gruppenebene außer Kraft setzen, wenn Traffic-Shaping aktiviert ist.



Es gibt folgende Policys, auf die die port-gruppenspezifischen Ausnahmen angewendet werden.

Diese Policy wird auf alle virtuellen Adapter angewendet, die an die Port-Gruppe angeschlossen sind, nicht jedoch auf den vSwitch selbst.

- **Status** – Wenn Sie die Policy-Ausnahmen im Feld **Status** aktivieren, begrenzen Sie den Umfang der Netzwerkbandbreitenzuweisung für jeden virtuellen Adapter, der der betreffenden Port-Gruppe zugeordnet ist. Wenn Sie die Policy deaktivieren, haben die Dienste standardmäßig freien, ungehinderten Zugang zum physischen Netzwerk.

Die übrigen Felder legen die Parameter für den Netzwerkdatenverkehr fest:

- **Durchschnittliche Bandbreite** – Ein Wert, der über einen bestimmten Zeitraum gemessen wird.
- **Spitzenbandbreite** – Ein Wert, der die zulässige Höchstbandbreite angibt. Dieser Wert muss größer als die durchschnittliche Bandbreite sein. Dieser Parameter begrenzt die Höchstbandbreite während eines Bursts.

- **Burstgröße** – Dieser Wert gibt an, wie groß ein Burst sein darf (in Kilobyte (KB)). Dieser Parameter steuert die Datenmenge, die während eines Bursts bei der Überschreitung der durchschnittlichen Datenübertragungsrate übertragen werden kann.

Policy für Lastenausgleich und Failover

Mit den Lastausgleichs- und Failover-Policys können Sie festlegen, wie der Netzwerk-Datenverkehr zwischen den Adaptern verteilt wird und wie der Verkehr neu geroutet wird, wenn ein Adapter ausfällt. Dazu müssen Sie die folgenden Parameter konfigurieren:

- Lastausgleichs-Policy

  Die Lastausgleichs-Policy legt fest, wie der ausgehende Datenverkehr über die Netzwerkadapter, die dem vSwitch zugewiesen wurden, verteilt wird.

HINWEIS Der eingehende Datenverkehr wird durch die Lastausgleichs-Policy auf dem physischen Switch gesteuert.

- Failover-Erkennung: Verbindungsstatus/Signalprüfung
- Reihenfolge der Netzwerkadapter (Aktiv/Standby)

Bearbeiten der Policy für Failover und Lastausgleich

1. Melden Sie sich am VMware VI Client an und wählen Sie den Server aus dem Inventar aus.

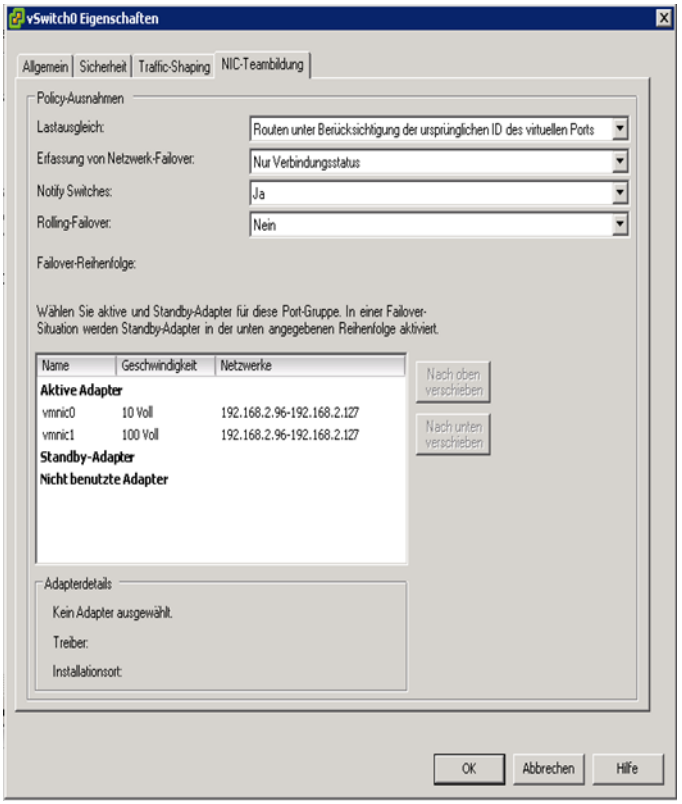
   Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

2. Klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Netzwerk**.
3. Markieren Sie einen vSwitch und klicken Sie auf **Bearbeiten**.
4. Klicken Sie im Dialogfeld **vSwitch-Eigenschaften** auf die Registerkarte **Ports**.
5. Markieren Sie den vSwitch und klicken Sie auf **Eigenschaften**, um die Werte für **Failover und Lastausgleich** für den vSwitch zu bearbeiten.

   Das Dialogfeld **Eigenschaften** für den vSwitch wird angezeigt.

6 Klicken Sie auf die Registerkarte **NIC-Teaming**.

Das Dialogfeld **Policy-Ausnahmen** wird angezeigt. Sie können den Failover-Befehl auf Port-Gruppenebene aussetzen. Standardmäßig werden neue Adapter für alle Policys auf „Aktiv“ gesetzt. Neue Adapter übertragen den Datenverkehr für den vSwitch und seine Port-Gruppe, wenn Sie nichts anderes angeben.



7 Im **Policy-Ausnahmen** Dialogfeld:

- **Lastenausgleich** – Geben Sie an, wie ein Uplink ausgewählt werden soll.
  - **Anhand der Quelle der Port-ID routen** – Der Uplink wird anhand des virtuellen Ports ausgewählt, an dem der Datenverkehr den virtuellen Switch ansteuert.
  - **Anhand des IP-Hashs routen** – Der Uplink wird anhand des Hashs der Ursprungs- und Ziel-IP-Adresse jedes Pakets ausgewählt. Bei Paketen ohne IP wird zur Berechnung des Hashs der Wert verwendet, der im Offset eingetragen ist.

- **Anhand des MAC-Hashs routen** – Der Uplink wird anhand des Hashs des Ursprungs-Ethernets ausgewählt.
- **Explizite Failover-Reihenfolge verwenden** – Es wird immer der Uplink ausgewählt, der im Verzeichnis der aktiven Adapter am weitesten oben steht und die Failover-Erkennungskriterien erfüllt.

- **Netzwerk-Failover-Erkennung** – Geben Sie die Verfahrensweise zur Verwendung der Failover-Erkennung an.
  - **Nur Verbindungsstatus** – Verlässt sich ausschließlich auf den vom Netzwerkadapter gemeldeten Verbindungsstatus. Hierdurch werden Ausfälle wie nicht angeschlossene Kabel oder Betriebsausfälle des physischen Switches erkannt, nicht jedoch Konfigurationsfehler wie z. B. Blockierung eines Ports des physischen Switches durch Spanning Tree, Zuweisung zum falschen VLAN oder nicht angeschlossene Kabel auf der anderen Seite des physischen Switches.
  - **Signalprüfung** – Sendet Signale und sucht nach Signalen auf allen NICs im Team und verwendet diese Informationen zusätzlich zum Verbindungsstatus, um einen Verbindungsausfall zu erkennen. Dadurch können viele der oben genannten Ausfälle erkannt werden, die durch den Verbindungsstatus allein nicht erkannt werden können.
- **Notify Switch** – Wählen Sie **Ja** oder **Nein**, um Failover an die Switches zu melden.

  Wenn Sie **Ja** wählen, wird jedes Mal, wenn eine virtuelle NIC an den vSwitch angeschlossen wird oder der Datenverkehr dieser virtuellen NIC aufgrund eines Failover-Ereignisses über eine andere physische NIC geroutet wird, eine Meldung über das Netzwerk gesendet, um die Verweistabelle auf dem physischen Switch zu aktualisieren. In fast allen Fällen ist dies wünschenswert, um die Latenzzeiten für Failover-Ereignisse und Migrationen mit VMotion zu minimieren.

HINWEIS Verwenden Sie diese Option nicht, wenn die an die Port-Gruppe angeschlossenen virtuellen Maschinen den Netzwerklastausgleich (NLB) von Microsoft im Unicast-Modus verwenden. Im Multicast-Modus von NLB treten keine Probleme auf.

- **Rolling-Failover** – Wählen Sie **Ja** oder **Nein**, um Rolling-Failover zu deaktivieren oder zu aktivieren.

  Diese Option bestimmt, wie ein physischer Adapter nach einem Ausfall wieder in den aktiven Betrieb genommen wird. Wenn die Option auf **Nein** gesetzt wurde, wird der Adapter sofort nach der Wiederherstellung seiner Funktionsfähigkeit aktiviert; er ersetzt in diesem Fall den ggf. vorhandenen Ersatzadapter, der seinen Platz eingenommen hatte. Wenn diese Option auf **Ja** gesetzt wurde, bleibt ein ausgefallener Adapter nach der Wiederherstellung

seiner Funktionsfähigkeit deaktiviert, bis der gegenwärtig aktive Adapter ausfällt und ersetzt werden muss.

- **Failover-Reihenfolge** – Geben Sie an, wie die Arbeitslast für die Adapter verteilt werden soll. Wenn Sie bestimmte Adapter verwenden und andere für Notfälle reservieren möchten, wenn die verwendeten Adapter ausfallen, können Sie Adapter mithilfe des Drop-Down-Menüs in zwei Gruppen aufteilen:
  - **Aktive Adapter** – Dieser Adapter wird weiter verwendet, wenn die Konnektivität des Netzwerkadapters besteht und aktiv ist.
  - **Standby-Adapter** – Dieser Adapter wird verwendet, wenn die Konnektivität eines der aktiven Adapter nicht besteht.
  - **Nicht verwendete Adapter** – Dieser Adapter soll nicht verwendet werden.

Konfigurieren der Port-Gruppe

Sie können die folgenden Port-Gruppen-Konfigurationen ändern:

- Port-Gruppen-Eigenschaften
- Gekennzeichnete Netzwerk-Policys

Bearbeiten der Eigenschaften von Port-Gruppen

1. Melden Sie sich am VMware VI Client an und wählen Sie den Server aus dem Inventar aus.

   Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

2. Klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Netzwerk**.
3. Klicken Sie auf der rechten Seite des Fensters für ein Netzwerk auf **Eigenschaften**.

   Das Dialogfeld **vSwitch-Eigenschaften** wird angezeigt.

4. Klicken Sie auf die Registerkarte **Ports**.
5. Markieren Sie eine Port-Gruppe und klicken Sie auf **Bearbeiten**.
6. Klicken Sie im Dialogfeld **Eigenschaften** der Port-Gruppe auf die Registerkarte **Allgemein**, um folgende Einstellungen zu ändern:
   - **Netzwerkbezeichnung** – Bezeichnet die Port-Gruppe, die erstellt wird. Geben Sie diese Bezeichnung ein, wenn Sie einen virtuellen Adapter zu dieser Port-Gruppe zuweisen, entweder bei der Konfiguration von virtuellen Maschinen oder von VMkernel-Diensten wie z. B. VMotion oder IP-Speicher.
   - **VLAN-ID** – Gibt das VLAN an, das für den Netzwerkdatenverkehr der Port-Gruppe verwendet wird.
7. Klicken Sie auf **OK**, um das Dialogfeld **vSwitch-Eigenschaften** zu verlassen.

So setzen Sie die Policys für bezeichnete Netzwerke außer Kraft

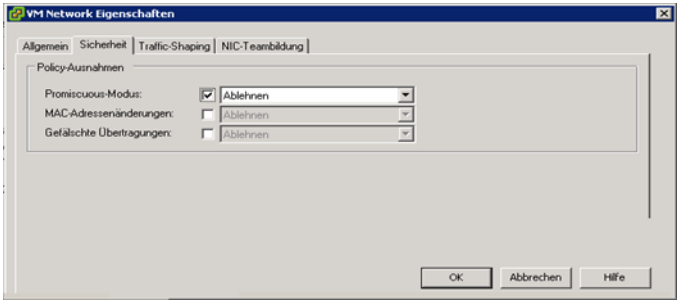
1 Um diese Einstellungen für ein bestimmtes bezeichnetes Netzwerk außer Kraft zu setzen, markieren Sie zuerst das Netzwerk.

2 Klicken Sie auf **Bearbeiten**.

3 Klicken Sie auf die Registerkarte **Sicherheit**.

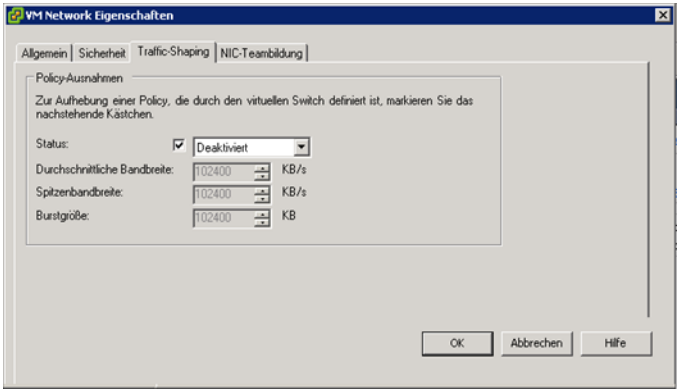
4 Aktivieren Sie das Kontrollkästchen für das bezeichnete Netzwerk, dass Sie außer Kraft setzen möchten.

Weitere Informationen zu diesen Einstellungen finden Sie unter „Sicherheits-Policy für Layer 2“ auf Seite 53.



5 Klicken Sie auf die Registerkarte **Traffic-Shaping**.

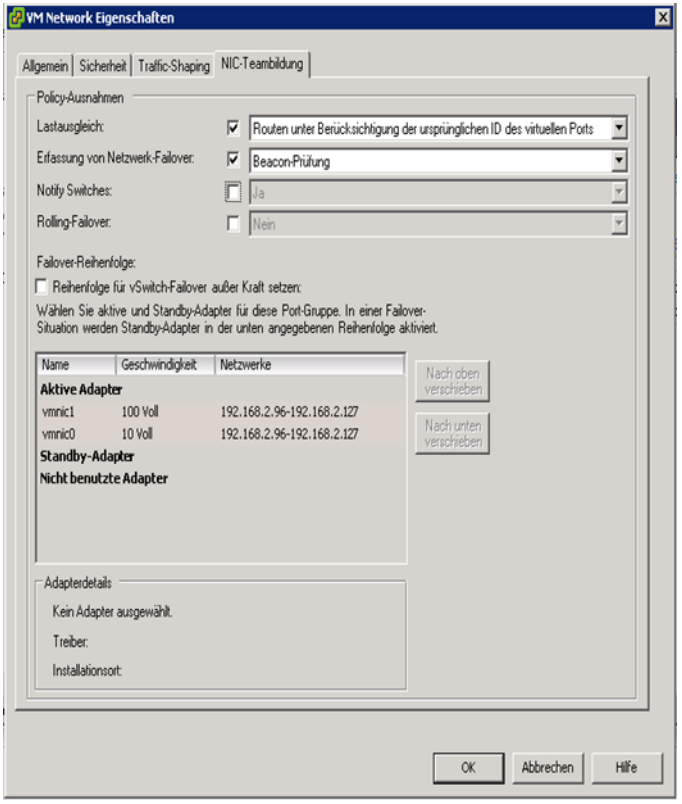
6 Markieren Sie das Kontrollkästchen, um den Aktiviert- oder Deaktiviert-**Status** außer Kraft zu setzen. Weitere Informationen zu den **Status**-Einstellungen finden Sie unter „Traffic-Shaping-Policy“ auf Seite 55.



7 Klicken Sie auf die Registerkarte **NIC-Teaming**.

8 Markieren Sie das zugeordnete Kontrollkästchen, um die Lastausgleichs- oder Policys für die Failover-Reihenfolge zu überschreiben.

Weitere Informationen zu diesen Einstellungen finden Sie unter „Policy für Lastenausgleich und Failover“ auf Seite 57.



9 Klicken Sie auf **OK**, um das Dialogfeld **VM-Netzwerkeigenschaften** zu schließen.

DNS und Routing

Konfigurieren Sie DNS und Routing über den VI Client.

Ändern der DNS- und Routing-Konfiguration

1 Melden Sie sich am VMware VI Client an und wählen Sie den Server aus dem Inventar aus.

Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration** und dort auf **DNS und Routing**.

3 Klicken Sie auf der rechten Bildschirmseite auf **Eigenschaften**.

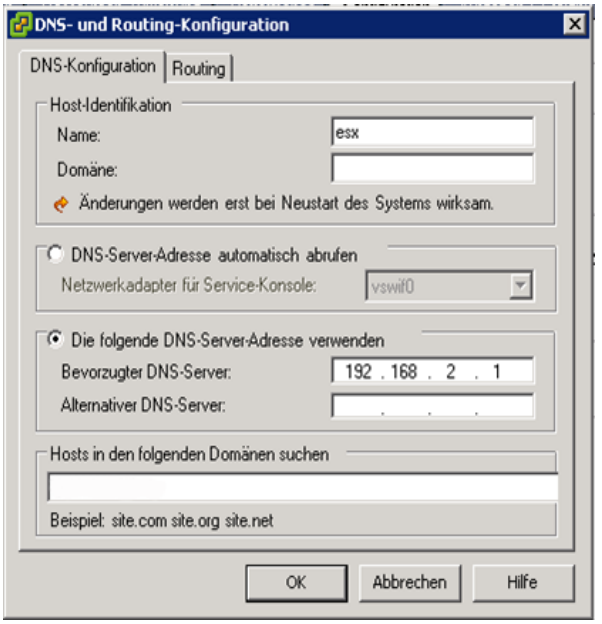
4 Geben Sie auf der Registerkarte **DNS-Konfiguration** die Werte für **Name** und **Domäne** ein.

5 Sie können die Adresse des DNS-Servers entweder automatisch beziehen oder eine DNS-Server-Adresse eingeben.

HINWEIS DHCP wird nur unterstützt, wenn die Servicekonsole auf den DHCP-Server zugreifen kann. Anders gesagt, für die Servicekonsole muss eine virtuelle Schnittstelle (vswif) konfiguriert und an das Netzwerk angeschlossen werden, in dem sich der DHCP-Server befindet.

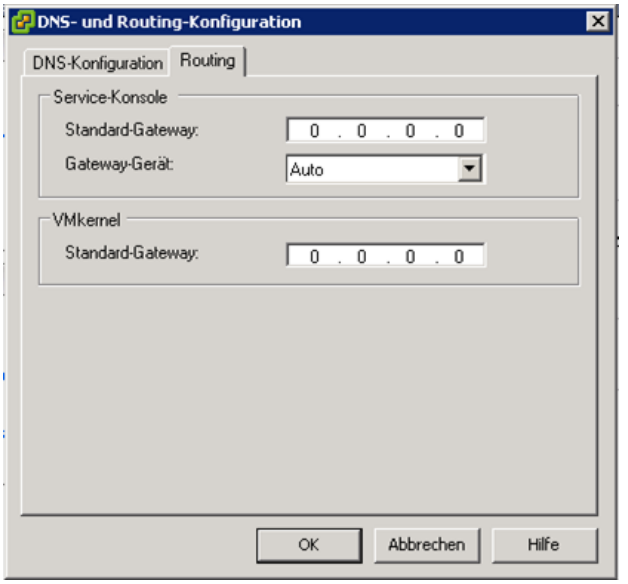
---

6 Geben Sie die Domänen an, in denen Hosts gesucht werden sollen.



7 Ändern Sie auf der Registerkarte **Routing** die Standard-Gateway nach Bedarf.

Sie müssen das Gateway-Gerät nur dann angeben, wenn die Servicekonsole auf mehr als ein Subnetz zugreifen soll.



8 Klicken Sie auf **OK**, um das Dialogfeld **DNS-Konfiguration** zu schließen.

Einrichten von MAC-Adressen

Für die von der Servicekonsole, dem VMkernel und den virtuellen Maschinen genutzten virtuellen Netzwerkadaptern werden MAC-Adressen generiert. In den meisten Fällen sind diese MAC-Adresse ausreichend. In folgenden Fällen ist es jedoch ggf. notwendig, eine MAC-Adresse für einen virtuellen Netzwerkadapter festzulegen:

- Virtuelle Netzwerkadapter auf unterschiedlichen physischen Servern verwenden das gleiche Subnetz und ihnen wurde die gleiche MAC-Adresse zugewiesen, wodurch ein Konflikt entsteht.
- Sie möchten sicherstellen, dass ein virtueller Netzwerkadapter immer die gleiche MAC-Adresse hat.

Die folgenden Abschnitte beschreiben, wie MAC-Adressen generiert werden und wie Sie die MAC-Adresse für einen virtuellen Netzwerkadapter festlegen können.

Generierung von MAC-Adressen

Jedem virtuellen Netzwerkadapter in einer virtuellen Maschine wird eine eindeutige MAC-Adresse zugewiesen. Eine MAC-Adresse ist eine Zahl bestehend aus sechs Byte. Jedem Hersteller von Netzwerkadaptern wird ein eindeutiges, drei Byte großes Präfix zugewiesen, das OUI (Organizationally Unique Identifier, eindeutiger Bezeichner für Organisationen) genannt wird und das der Hersteller zur Generierung von eindeutigen MAC-Adressen verwenden kann.

VMware verfügt über drei OUIs:

- OUI für generierte MAC-Adressen.
- OUI für manuell festgelegte MAC-Adressen.
- OUI für ältere virtuelle Maschinen; dieser OUI wird jedoch bei ESX Server 3.0 nicht mehr verwendet.

Die ersten drei Byte der MAC-Adresse, die für jeden virtuellen Netzwerkadapter generiert werden, haben diesen Wert. Der Generierungsalgorithmus für MAC- Adressen erstellt drei weitere Byte. Der Algorithmus garantiert eindeutige MAC-Adressen in einer Maschine und versucht, eindeutige MAC-Adressen für mehrere Maschinen zu erstellen.

Die Netzwerkadapter für jede virtuelle Maschine im gleichen Subnetz sollten eindeutige MAC-Adressen haben. Im anderen Fall können sie sich unvorhersehbar verhalten. Der Algorithmus beschränkt jederzeit auf allen Servern die Anzahl der laufenden und angehaltenen virtuellen Maschinen. Er kann auch nicht alle Fälle von gleichen MAC-Adressen vermeiden, wenn sich virtuelle Maschinen auf unterschiedlichen physischen Computern ein Subnetz teilen.

Der VMware UUID (Universally Unique Identifier, universaler eindeutiger Bezeichner) generiert MAC-Adressen, die dann auf Konflikte geprüft werden. Die generierten MAC-Adressen werden aus drei Teilen erstellt: aus der VMware OUI, der SMBIOS-UUID für den physischen ESX Server und einem Hash, der auf dem Namen der Organisation beruht, für die die MAC-Adresse generiert wird.

Wenn die MAC-Adresse generiert wurde, ändert sie sich nicht, solange die virtuelle Maschine nicht an einen anderen Speicherort verschoben wird, z. B. in ein anderes Verzeichnis auf dem gleichen Server. Die MAC-Adresse in der Konfigurationsdatei der virtuellen Maschine wird gespeichert. Alle MAC-Adressen, die Netzwerkadaptern von laufenden oder angehaltenen virtuellen Maschinen auf einem bestimmten physischen Computer zugewiesen wurden, werden kontrolliert.

Die MAC-Adresse einer ausgeschalteten virtuellen Maschine wird nicht gegen die MAC-Adressen von laufenden oder angehaltenen virtuellen Maschinen geprüft. Es ist möglich, aber unwahrscheinlich, dass beim Hochfahren einer virtuellen Maschine eine andere MAC-Adresse angefordert wird. Diese Anforderung wird durch einen Konflikt mit einer virtuellen Maschine verursacht, die hochgefahren wurde, während diese virtuelle Maschine ausgeschaltet war.

Einstellen von MAC-Adressen

Um die Begrenzung auf 256 virtuelle Netzwerkadapter pro physischen Computer zu umgehen und mögliche MAC-Adressenkonflikte zwischen virtuellen Maschinen zu vermeiden, können Systemadministratoren MAC-Adressen manuell zuweisen. VMware verwendet folgenden OUI für manuell generierte MAC-Adressen: 00:50:56.

Der Adressbereich für die MAC-Adresse lautet

```
00:50:56:00:00:00–00:50:56:3F:FF:FF
```

Sie können die Adressen einstellen, indem Sie der Konfigurationsdatei der virtuellen Maschine folgende Zeile hinzufügen:

```
ethernet <Nummer>.address = 00:50:56:XX:YY:ZZ
```

wobei `<number>` die Zahl des Ethernet-Adapters angibt, `XX` eine gültige Hexadezimalzahl zwischen 00 und 3F ist und `YY` und `ZZ` gültige Hexadezimalzahlen zwischen 00 und FF sind. Der Wert für `XX` darf nicht größer als 3F sein, um Konflikte mit MAC-Adressen zu vermeiden, die von VMware Workstation und VMware GSX Server generiert werden. Der Höchstwert für eine manuell generierte MAC-Adresse lautet

```
ethernet<Nummer>.address = 00:50:56:3F:FF:FF
```

Sie müssen außerdem folgende Option in der Konfigurationsdatei der virtuellen Maschine setzen:

```
ethernet<Nummer>.addressType="static"
```

Da virtuelle Maschinen von VMware ESX Server keine willkürlichen MAC-Adressen unterstützen, muss das oben genannte Format eingehalten werden. Wenn Sie für Ihre nicht veränderlichen Adressen einen einzigartigen Wert für `XX:YY:ZZ` festlegen, dürften keine Konflikte zwischen den automatisch zugewiesenen und den manuell zugewiesenen MAC-Adressen auftreten.

Verwendung von MAC-Adressen

Um sich mit MAC-Adressen vertraut zu machen, richten Sie einfach eine MAC-Adresse ein.

So richten Sie eine MAC-Adresse ein

1. Legen Sie fest, dass die MAC-Adresse statisch ist.
2. Löschen Sie folgende Optionen aus der Konfigurationsdatei der virtuellen Maschine:

   ```
   ethernet<Nummer>.address, ethernet<Nummer>.addressType
   ```

   und

   ```
   ethernet<Nummer>.generatedAddressOffset
   ```

3. Überprüfen Sie, dass der virtuellen Maschine eine generierte MAC-Adresse zugewiesen wurde.

VMware garantiert durch die Verwendung der VMware OUIs (00:0C:29 und 00:50:56), die nur für virtuelle Maschinen gelten, dass die MAC-Adresse niemals mit physischen Hosts in Konflikt gerät.

Netzwerk-Tipps und Empfehlungen

In diesem Abschnitt finden Sie Informationen zu folgenden Themen:

- Netzwerkempfehlungen
- Netzwerk-Tipps

Netzwerkempfehlungen

Ziehen Sie folgende Empfehlungen für die Konfiguration Ihres Netzwerkes in Betracht:

- Trennen Sie die Netzwerkdienste voneinander, um bessere Sicherheit und höhere Leistung zu erreichen.

  Wenn eine bestimmte Gruppe virtueller Maschinen höchste Leistung bieten soll, schließen Sie sie an eine eigene physische NIC an. Durch diese Abtrennung kann ein Teil der Gesamtarbeitslast des Netzwerkes gleichmäßiger über mehrere CPUs verteilt werden. Die isolierten virtuellen Maschinen sind dann besser in der Lage, z. B. den Datenverkehr eines Webclients zu verarbeiten.

- Die unten aufgeführten Empfehlungen können entweder durch die Verwendung von VLANs zur Aufteilung eines physischen Netzwerkes in Segmente oder durch die Verwendung getrennter physischer Netzwerke umgesetzt werden (die zweite Variante ist dabei zu bevorzugen).

  - Ein wichtiger Bestandteil der Absicherung des ESX-Systems besteht darin, dass die Servicekonsole über ein eigenes Netzwerk verfügt. Die Netzwerkanbindung der Servicekonsole sollte genauso gehandhabt werden wie Geräte für den Fernzugriff auf Server, da die Übernahme der Servicekonsole einem Angreifer die vollständige Kontrolle über alle virtuellen Maschinen auf dem System ermöglicht.

  - Es ist wichtig, dass die VMotion-Verbindung über ein eigenes, für diesen Zweck vorgesehenes Netzwerk verfügt, da die Speicherinhalte des Gast-Betriebssystems bei der Migration mit VMotion über das Netzwerk übertragen werden.

Einbindung von NAS-Datenträgern

Die Art und Weise, wie der ESX Server 3.0 auf NFS-Speicher von ISO-Images, die als virtuelle CD-ROMs für virtuelle Maschinen verwendet werden, zugreift, unterscheidet sich von der Weise, wie das beim ESX Server 2.x geschah.

ESX Server 3.0 unterstützt die VMkernel-basierte NFS-Einbindung. Bei dem neuen Einbindungsmodell wird der NFS-Datenträger mit den ISO-Images über die NFS-Funktion des VMkernels eingebunden. Alle so eingebundenen NFS-Datenträger werden im VI Client als Datastores angezeigt. Mit dem Konfigurationseditor der virtuellen Maschinen können Sie das Dateisystem der Servicekonsole nach ISO-Images durchsuchen, die als virtuelle CD-ROM-Laufwerke verwendet werden sollen.

Netzwerk-Tipps

Beachten Sie auch die folgenden Netzwerkhinweise:

- Netzwerkdienste können am einfachsten physisch getrennt und eine bestimmte Gruppe von NICs einem bestimmten Netzwerkdienst zugewiesen werden, indem ein vSwitch für jeden Dienst erstellt wird. Wenn das nicht möglich ist, können die Dienste auf einem vSwitch voneinander getrennt werden, indem sie an Port-Gruppen mit unterschiedlichen VLAN-IDs angeschlossen werden. In jeden Fall sollte der Netzwerkadministrator überprüfen, dass die gewählten Netzwerke oder VLANs vom Rest der Umgebung isoliert sind, d. h. dass keine Router daran angeschlossen sind.
- Sie können NICs zum vSwitch hinzufügen oder davon entfernen, ohne dass die virtuellen Maschinen oder die Netzwerkdienste hinter diesem vSwitch beeinflusst werden. Wenn Sie die gesamte Hardware entfernen, können die virtuellen Maschinen immer noch untereinander kommunizieren, als würden sie ins Netz und wieder zurück gehen. Wenn eine NIC verblieben ist, können alle virtuellen Maschinen noch auf das physische Netzwerk zugreifen.
- Verwenden Sie Port-Gruppen mit verschiedenen aktiven Adaptergruppen in der Teaming-Policy, um virtuelle Maschinen in Gruppen einzuteilen. Diese Gruppen können unterschiedliche Adapter verwenden, wenn alle Adapter funktionsfähig sind. Im Fall eines Netzwerk- oder Hardware-Ausfalls teilen sie sich die Adapter jedoch wieder.
- Installieren Sie Firewalls auf virtuellen Maschinen, die Datenverkehr zwischen virtuellen Netzwerken mit Uplinks zu physischen Netzwerken und reinen virtuellen Netzwerken ohne Uplinks vermitteln, um die empfindlichsten virtuellen Maschinen zu schützen.

Netzwerk-Szenarien und Problemlösung

4

Dieses Kapitel beschreibt die allgemeine Netzwerkkonfiguration und Problemlösungsszenarios.

In diesem Kapitel werden folgende Themen behandelt:

- „Netzwerkkonfiguration für den Software iSCSI Speicher“ auf Seite 70
- „Konfiguration des Netzwerks auf Blade-Servern“ auf Seite 76
- „Problemlösungen“ auf Seite 80

Netzwerkkonfiguration für den Software iSCSI Speicher

Der Speicher, den Sie für einen ESX Server-Host konfigurieren, kann ein oder Storage Area Networks (SAN) umfassen, die iSCSI verwenden, wobei es sich um ein Mittel zum Zugriff auf die SCSI-Geräte und zum Austausch der Datenprotokolle handelt, das TCP/IP-Protokolle über einen Netzwerk-Port und nicht über einen direkten Anschluss an ein SCSI-Gerät einsetzt. In iSCSI-Übertragungen werden Raw-SCSI-Datenblöcke in iSCSI-Berichte eingekapselt und an das Gerät oder den Anwender, der die Anfrage gestellt hat, übertragen.

Bevor Sie den iSCSI-Speicher konfigurieren können, müssen Sie einen VMkernel-Port für das iSCSI-Netzwerk und die Verbindung der Servicekonsole zum iSCSI-Netzwerk anlegen.

Anlegen eines VMkernel-Ports für Software-iSCSI

1 Melden Sie sich am VMware VI Client an und wählen Sie den Server aus dem Inventarnfenster aus.

   Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Netzwerk**.

3 Klicken Sie auf den Link **Netzwerk hinzufügen**.

   Der **Assistent zum Hinzufügen von Netzwerken** wird angezeigt.

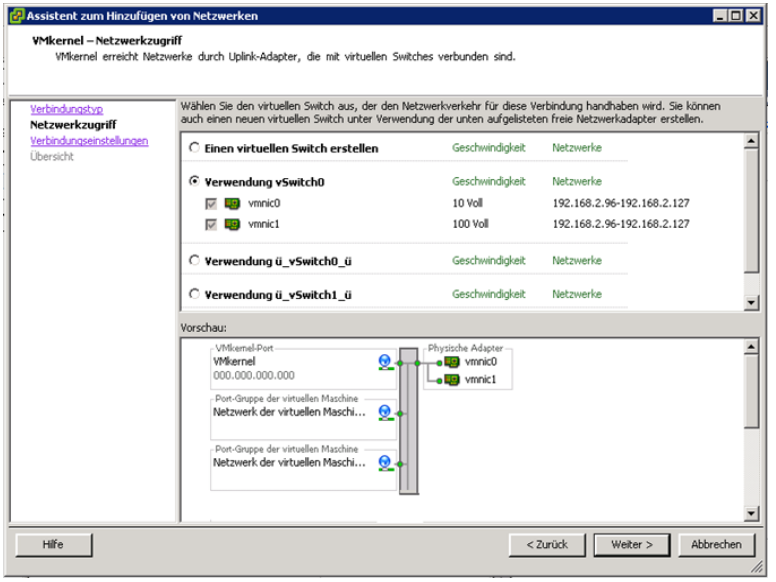
4 Wählen Sie **VMkernel** und klicken Sie auf **Weiter**.

   Damit können Sie den VMkernel, der die Dienste für den iSCSI-Speicher ausführt, an das physische Netzwerk anschließen.

   Das Dialogfeld **Netzwerkzugang** wird angezeigt.

5 Wählen Sie den vSwitch aus, den Sie verwenden möchten, oder aktivieren Sie das Optionsfeld **Einen virtuellen Switch erstellen**.

6 Aktivieren Sie die Kontrollkästchen für die Netzwerkadapter, die Ihr vSwitch verwenden soll.



Die Auswahlmöglichkeiten werden im Bereich **Vorschau** angezeigt.

Wählen Sie für jeden vSwitch Adapter aus, sodass die virtuellen Maschinen, die an diesen Adapter angeschlossen sind, auf das richtige Ethernet-Segment zugreifen können. Wenn unter **Neuen virtuellen Switch erstellen** keine Adapter angezeigt werden, bedeutet dies, dass alle Netzwerkadapter im System von vorhandenen vSwitches verwendet werden.

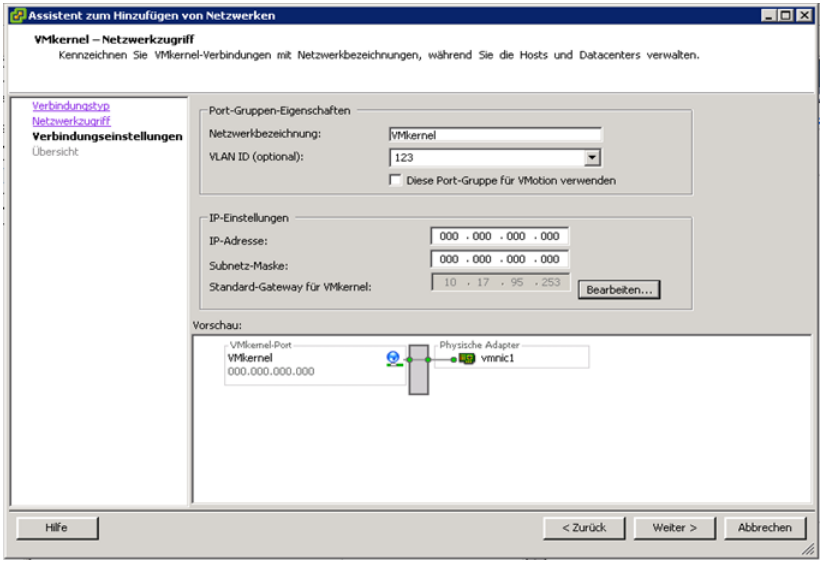
Weiter Informationen zum Bewegen von Netzwerkadapter zwischen vSwitches finden Sie unter „Hinzufügen von Uplink-Adaptern“ auf Seite 50.

7 Klicken Sie auf **Weiter**.

Das Dialogfeld **Verbindungseinstellungen** wird angezeigt.

8 Wählen Sie eine Netzwerkbezeichnung und eine VLAN-ID unter **Eigenschaften der Port-Gruppe** aus bzw. geben Sie diese ein.

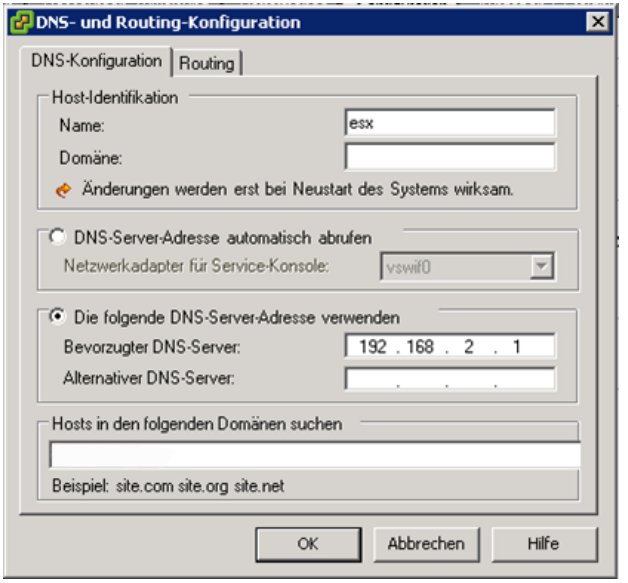
- **Netzwerkbezeichnung** – Ein Name, der die Port-Gruppe bezeichnet, die erstellt wird. Es handelt sich dabei um die Bezeichnung, die Sie bei der Konfiguration eines virtuellen Adapters, der an diese Port-Gruppe angeschlossen wird, beim Konfigurieren eines iSCSI-Speichers festlegen.
- **VLAN-ID** – Bezeichnet das VLAN, das für den Netzwerkdatenverkehr der Port-Gruppe verwendet wird.



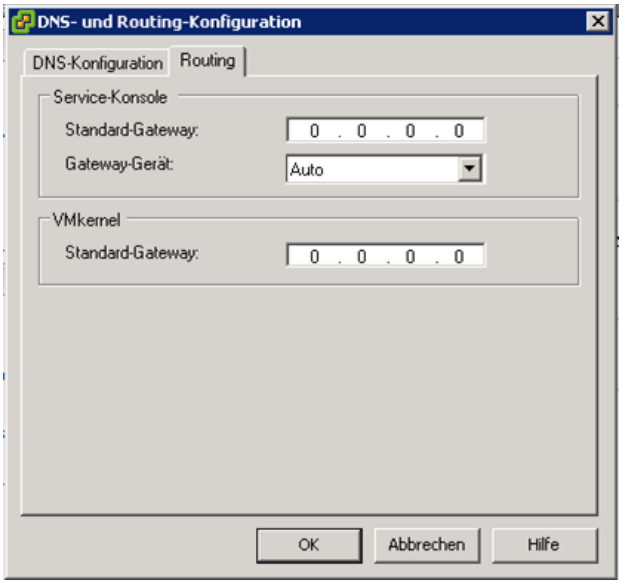
9 Unter **IP-Einstellungen** klicken Sie auf **Bearbeiten**, um den **VMkernel-Standardgateway** für iSCSI anzugeben.

Das Dialogfeld **DNS und Routing-Konfiguration** wird angezeigt. Auf der Registerkarte **DNS-Konfiguration** ist im Namensfeld standardmäßig der Hostname eingetragen.

Auch die DNS-Server-Adressen und die Domäne, die während der Installation angegeben wurden, werden automatisch ausgefüllt.



Auf der Registerkarte **Routing** benötigen die Servicekonsole und das VMkernel jeweils eigene Gateway-Angaben. Eine Gateway ist zur Anbindung an Computer notwendig, die sich nicht im gleichen IP-Subnetz wie die Servicekonsole oder das VMkernel befinden.



HINWEIS Die Standard-Gateway für den Port, den Sie erstellen, muss eingestellt werden. Sie müssen eine gültige statische IP-Adresse angeben, um den VMkernel-Stapel zu konfigurieren.

10 Klicken Sie auf **OK**, um die Änderungen zu speichern und schließen Sie das Dialogfeld **DNS und Routing-Konfiguration**.

11 Klicken Sie auf **Weiter**.

12 Wenn Sie Änderungen vornehmen möchten, verwenden Sie die Schaltfläche **Zurück**.

13 Überprüfen Sie die Änderungen im Dialogfeld **Fertig stellen** und klicken Sie auf **Fertig stellen**.

Nach dem Anlegen des VMkernel-Ports für iSCSI, müssen Sie eine Verbindung der Servicekonsole auf demselben vSwitch anlegen, auf dem der VMkernel-Port ist.

Anlegen einer Verbindung der Servicekonsole zum iSCSI-Software-Speicher

1 Melden Sie sich am VMware VI Client an und wählen Sie den Server aus dem Inventar aus.

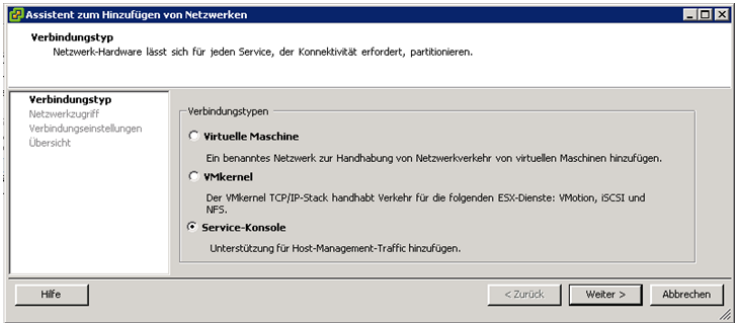
Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Netzwerk**.

3 Auf der rechten Seite des Bildschirms klicken Sie auf **Eigenschaften** für den vSwitch, der dem VMkernel-Port zugeordnet ist, den Sie gerade angelegt haben.

4 In der Registerkarte **Port** klicken Sie auf **Hinzufügen**.

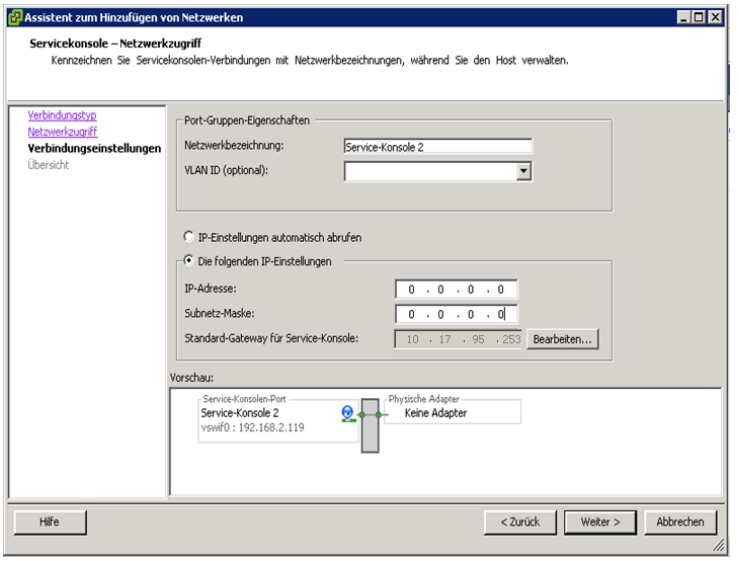
Der **Assistent zum Hinzufügen von Netzwerken** wird angezeigt.



5 Wählen Sie als Verbindungsart **Servicekonsole** und klicken Sie auf **Weiter**.

Das Dialogfeld **Verbindungseinstellungen** wird angezeigt.

6 Geben Sie unter **Eigenschaften der Port-Gruppe** eine Netzwerkbezeichnung für die zu erstellende Port-Gruppe ein.



Neuere Ports und Port-Gruppen werden im vSwitch-Diagramm oben angezeigt.

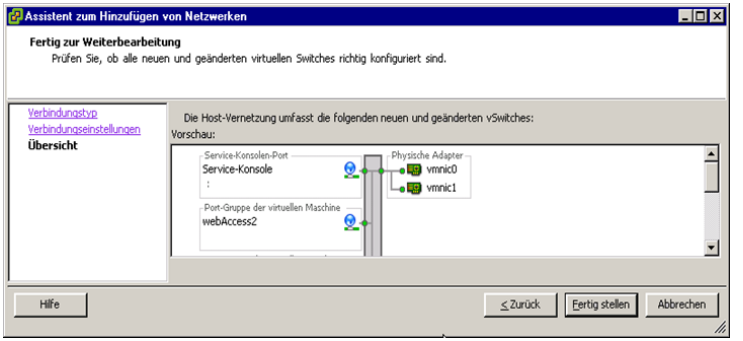
7 Geben Sie die **IP-Adresse** und die **Subnetzmaske** ein oder aktivieren Sie die DHCP-Option **IP-Einstellung automatisch beziehen** für die IP-Adresse und die Subnetzmaske.

8 Klicken Sie auf die Schaltfläche **Bearbeiten**, um die **Standard-Gateway der Servicekonsole** einzustellen.

Siehe „Einstellung der Standard-Gateway“ auf Seite 41.

9 Klicken Sie auf **Weiter**.

Das Dialogfeld **Fertig stellen** wird angezeigt.



10 Überprüfen Sie die Konfiguration des vSwitches noch einmal und klicken Sie dann auf **Fertig stellen**.

Nachdem Sie einen VMkernel-Port und die Servicekonsolen-Verbindung erstellt haben, können Sie den iSCSI-Software-Speicher aktivieren und konfigurieren. Weitere Informationen zur Konfiguration von iSCSI-Adaptern und Speichern finden Sie unter „iSCSI-Speicher“ auf Seite 110.

Konfiguration des Netzwerks auf Blade-Servern

Da Blade-Server mitunter nur über eine begrenzte Anzahl von Netzwerkadaptern verfügen, wird es wahrscheinlich erforderlich, VLANs für einen separaten Datenverkehr für die Servicekonsole, VMotion, den IP-Speicher und verschiedene Gruppen aus VMs zu verwenden. VMware Best-Practices-Methoden empfehlen Ihnen, aus Sicherheitsgründen eigene Netzwerke für die Servicekonsole und VMotion anzulegen. Wenn Sie eigenen vSwitches zu diesem Zweck physische Adapter zuweisen, müssen Sie möglicherweise auf redundante (geteamte) Verbindungen oder die Isolierung der verschiedenen Netzwerk-Clients oder auf beides verzichten. Mit VLANs können Sie eine Netzwerkbereitstellung erreichen, ohne mehrere physische Adapter verwenden zu müssen.

Damit der Netzwerk-Blade eines Blade-Servers die ESX Server-Port-Gruppe mit einem VLAN-getaggten Datenverkehr unterstützt, müssen sie das Blade so konfigurieren, dass es 802.1Q unterstützt und den Port als getaggten Port konfigurieren.

Die Methode zum Konfigurieren eines Ports als getaggten Port ist von Server zu Server verschieden. Die folgende Liste beschreibt die Konfiguration eines getaggten Ports auf drei der am häufigsten verwendeten Blade-Servern:

- **HP-Blade** – Setzt das **VLAN-Tagging** auf **Aktiviert**.
- **Dell PowerEdge** – Setzt den Port auf **Getagged**.
- **IBM eServer Blade Center** – Markieren Sie **Tag** in der Port-Konfiguration.

Konfigurieren einer Port-Gruppe für virtuelle Maschinen mit VLAN auf einem Blade-Server

1 Melden Sie sich am VMware VI Client an und wählen Sie den Server aus dem Inventar aus.

Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Netzwerk**.

3 Auf der rechten Seite des Bildschirms klicken Sie auf **Eigenschaften** für den vSwitch, der der Servicekonsole zugeordnet ist.

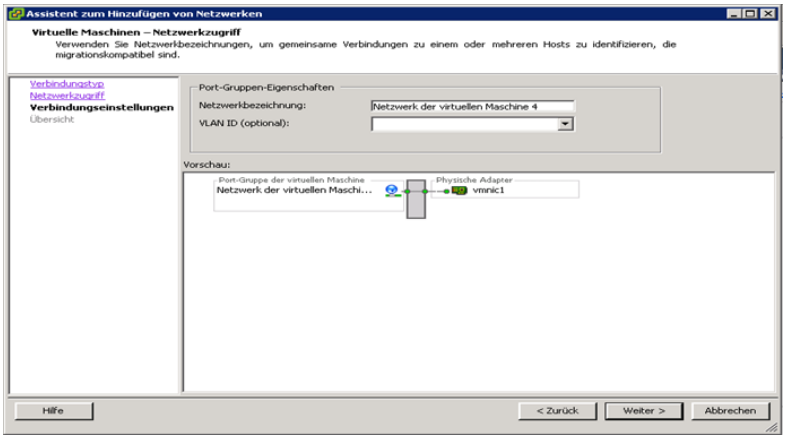
4 In der Registerkarte **Port** klicken Sie auf **Hinzufügen**.

Der **Assistent zum Hinzufügen von Netzwerken** wird angezeigt.

5 Wählen Sie als Verbindungsart **Virtuelle Maschinen** (Standardeinstellung).

6 Klicken Sie auf **Weiter**.

Das Dialogfeld **Verbindungseinstellungen** wird angezeigt.



7 Geben Sie unter **Eigenschaften der Port-Gruppe** eine Netzwerkbezeichnung für die zu erstellende Port-Gruppe ein.

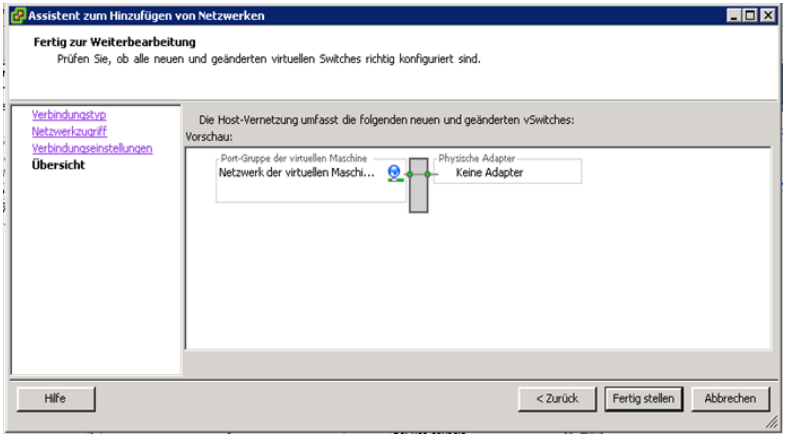
Mit den Netzwerkbezeichnungen können Sie migrationsfähige Verbindungen für zwei oder mehr Hosts identifizieren.

8 Geben Sie im **VLAN-ID**-Feld eine Zahl zwischen 1 und 4094 ein.

Wenn Sie sich nicht sicher sind, was hier eingegeben werden muss, lassen Sie das Feld frei oder wenden Sie sich an Ihren Netzwerkadministrator.

9 Klicken Sie auf **Weiter**.

Das Dialogfeld **Fertig stellen** wird angezeigt.



10 Überprüfen Sie die Konfiguration des vSwitches noch einmal und klicken Sie dann auf **Fertig stellen**.

Konfigurieren eines VMkernel-Ports mit VLAN auf einem Blade-Server

1 Melden Sie sich am VMware VI Client an und wählen Sie den Server aus dem Inventar aus.

Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Netzwerk**.

3 Auf der rechten Seite des Bildschirms klicken Sie auf **Eigenschaften** für den vSwitch, der der Servicekonsole zugeordnet ist.

4 In der Registerkarte **Port** klicken Sie auf **Hinzufügen**.

Der **Assistent zum Hinzufügen von Netzwerken** wird angezeigt.

5 Wählen Sie **VMkernel** und klicken Sie auf **Weiter**.

Damit können Sie das VMkernel, das Dienste für VMotion und IP-Speicher (NFS oder iSCSI) ausführt, an ein physisches Netzwerk anschließen.

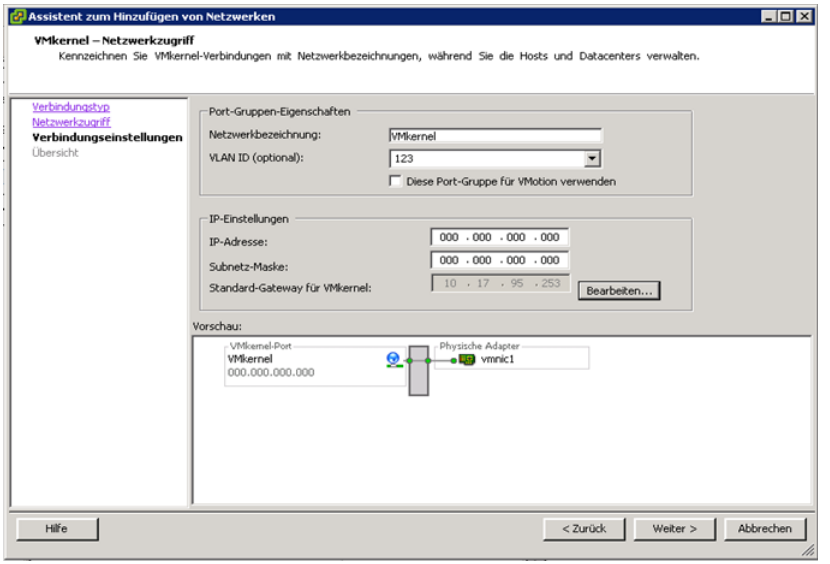
Das Dialogfeld **Verbindungseinstellungen** wird angezeigt.

6 Wählen Sie eine Netzwerkbezeichnung und eine VLAN-ID unter **Eigenschaften der Port-Gruppe** aus bzw. geben Sie diese ein.

- **Netzwerkbezeichnung** – Ein Name, der die Port-Gruppe bezeichnet, die erstellt wird. Es handelt sich dabei um die Bezeichnung, die Sie bei der Konfiguration von VMkernel-Diensten wie VMotion und IP-Speicher während der Konfiguration des virtuellen Adapters, der an diese Port-Gruppe angeschlossen wird, festlegen.
- **VLAN-ID** – Bezeichnet das VLAN, das für den Netzwerkdatenverkehr der Port-Gruppe verwendet wird.

7 Aktivieren Sie das Kontrollkästchen **Diese Port-Gruppe für VMotion verwenden**, damit diese Port-Gruppe anderen ESX Servern melden kann, dass sie die Netzwerkverbindung ist, an die VMotion-Datenverkehr gesendet werden soll.

Auf jedem ESX Server-Host kann diese Eigenschaft nur für eine VMotion- und IP-Speicher-Port-Gruppe aktiviert werden. Wenn diese Eigenschaft für keine der Port-Gruppen aktiviert wurde, ist eine VMotion-Migration auf diesen Host nicht möglich.



8 Klicken Sie unter **IP-Einstellungen** auf **Bearbeiten**, um das **Standard-Gateway für VMkernel** für VMkernel-Dienste wie z. B. VMotion, NAS und iSCSI einzurichten.

HINWEIS Die Standard-Gateway für den Port, den Sie erstellen, muss eingestellt werden. VirtualCenter 2 unterscheidet sich hier von VirtualCenter 1.x. Sie müssen zur Konfiguration des VMkernel-IP-Stapels eine gültige IP-Adresse verwenden, keine Pseudoadresse.

Das Dialogfeld **DNS und Routing-Konfiguration** wird angezeigt. Auf der Registerkarte **DNS-Konfiguration** ist im Namensfeld standardmäßig der Hostname eingetragen. Auch die DNS-Server-Adressen und die Domäne, die während der Installation angegeben wurden, werden automatisch ausgefüllt.

Auf der Registerkarte **Routing** benötigen die Servicekonsole und das VMkernel jeweils eigene Gateway-Angaben. Eine Gateway ist zur Anbindung an Computer notwendig, die sich nicht im gleichen IP-Subnetz wie die Servicekonsole oder das VMkernel befinden.

Standardmäßig ist „Statische IP“ eingestellt.

9 Klicken Sie auf **OK**, um die Änderungen zu speichern und schließen Sie das Dialogfeld **DNS-Konfiguration und Routing**.

10 Klicken Sie auf **Weiter**.

11 Wenn Sie Änderungen vornehmen möchten, verwenden Sie die Schaltfläche **Zurück**.

12 Überprüfen Sie die Änderungen im Dialogfeld **Fertig stellen** und klicken Sie auf **Fertig stellen**.

Problemlösungen

Der folgende Abschnitt führt Sie durch die Problemlösungen bei typischen Netzwerkproblemen.

In diesem Abschnitt werden folgende Themen behandelt:

- „Fehlerbehebung bei der Vernetzung der Servicekonsole“ auf Seite 80
- „Problemlösungen Netzwerkadapter-Konfiguration“ auf Seite 82
- „Problemlösungen Konfiguration physischer Switches“ auf Seite 82
- „Problemlösungen Port-Gruppen-Konfiguration“ auf Seite 82

Fehlerbehebung bei der Vernetzung der Servicekonsole

Wenn bestimmte Teile der Netzwerkkonfiguration der Servicekonsole falsch konfiguriert sind, können Sie über den VI Client nicht mehr auf den ESX Server-Host zu-

greifen. In diesem Fall können Sie die Netzwerkeinstellungen neu konfigurieren, indem Sie direkt auf die Servicekonsole zugreifen. Für SSH gibt es folgende Befehle:

- `esxcfg-vswif -l`

  Gibt eine Liste der bestehenden Netzwerkschnittstellen der Servicekonsole aus.

  Prüfen Sie, ob `vswif0` vorhanden ist und die aktuelle IP-Adresse und Netmask stimmen.

- `esxcfg-vswitch -l`

  Gibt eine Liste der bestehenden Konfigurationen für die virtuellen Switches aus.

  Prüfen Sie, ob der Uplink-Adapter, der für die Servicekonsole konfiguriert wurde, mit dem geeigneten physischen Netzwerk verbunden ist.

- `exscfg-nics -l`

  Gibt eine Liste der aktuellen Netzwerkadapter aus.

  Prüfen Sie, ob der Uplink-Adapter, der für die Servicekonsole konfiguriert wurde, läuft und ob Geschwindigkeit und Duplex stimmen.

- `esxcfg-nics -s <speed> <nic>`

  Ändert die Geschwindigkeit eines Netzwerkadapters.

- esxcfg-nics -d <duplex> <nic>

  Ändert den Duplex eines Netzwerkadapters.

- `esxcfg-vswif -i <neue IP-Adresse> vswifX`

  Ändert die IP-Adresse der Servicekonsole.

- `esxcfg-vswif -n <neue Subnetzmaske> vswifX`

  Ändert die Subnetzmaske der Servicekonsole.

- `esxcfg-vswitch -U <old vmnic> <service console vswitch>`

  Entfernt den Uplink für die Servicekonsole

- `esxcfg-vswitch -L <new vmnic> <service console vswitch>`

  Ändert den Uplink für die Servicekonsole.

Wenn Sie bei `esxcfg-*` Befehlen lang warten müssen, kann dies an einer falschen DNS-Einstellung liegen. Die `esxcfg-*` Befehle setzen voraus, dass DNS so konfiguriert ist, dass die Namensauflösung des lokalen Servers ordnungsgemäß funktioniert. Dies setzt wiederum voraus, dass die `/etc/hosts`-Datei einen Eintrag für die konfigurierte IP-Adresse und die Adresse 127.0.0.1 des lokalen Servers enthält.

Problemlösungen Netzwerkadapter-Konfiguration

Das Hinzufügen eines neuen Netzwerkadapters kann in bestimmten Fällen zum Verlust der Servicekonsolen-Konnektivität und der Verwaltungs- und Wartungsfreundlichkeit mit dem VI Client führen, was daran liegt, dass die Netzwerkadapter neu benannt werden.

Wenn dies der Fall ist, müssen Sie die betroffenen Netzwerkadapter, die die Servicekonsole nutzen, umbenennen.

Umbenennen der Netzwerkadapter, die die Servicekonsole verwenden

1. Melden Sie sich direkt an Ihrer ESX Server-Konsole an.
2. Verwenden Sie den Befehl `esxcfg-nics -l`, um sich anzeigen zu lassen, welche Namen Ihren Netzwerkadaptern zugewiesen wurden.
3. Verwenden Sie den Befehl `esxcfg-vswitch -l`, um sich anzeigen zu lassen, welche vSwitches, sofern überhaupt, jetzt den Gerätenamen zugewiesen sind, die nicht mehr durch esxcfg-nics angezeigt werden.
4. Verwenden Sie den Befehl `esxcfg-vswitch -U <old vmnic name> <vswitch>`, um Netzwerkadapter zu entfernen, die umbenannt worden sind.
5. Verwenden Sie den Befehl `esxcfg-vswitch -L <new vmnic name> <vswitch>`, um die Netzwerkadapter wieder hinzuzufügen und geben Sie Ihnen dabei die richtigen Namen.

Problemlösungen Konfiguration physischer Switches

In manchen Fällen kann es bei einem Failover oder Failback zu einem Verlust der vSwitch-Konnektivität kommen. Dies führt dazu, dass die MAC-Adressen, die die virtuellen Maschinen verwenden, die diesem vSwitch zugeordnet sind, auf einem anderen Switch-Port erscheinen als zuvor.

Um dieses Problem zu vermeiden, setzen Sie Ihren physischen Swicth auf den **Portfast** oder **Portfast-Trunk** Modus.

Problemlösungen Port-Gruppen-Konfiguration

Das Umbenennen einer Port-Gruppe bei bereits mit dieser Port-Gruppe verbundenen virtuellen Maschinen kann dazu führen, dass die Netzwerkkonfiguration der virtuellen Maschinen, die so konfiguriert sind, dass sie sich mit dieser Port-Gruppe verbinden, nicht mehr stimmt.

Die Verbindung von virtuellen Netzwerkadaptern mit den Port-Gruppen erfolgt über den Namen und der Name wird in der virtuellen Maschinen-Konfiguration gespeichert. Das Ändern des Namens einer Port-Gruppe führt nicht zu einer Massen-Neukonfiguration aller virtuellen Maschinen, die mit dieser Port-Gruppe verbunden sind. Virtuelle Maschinen, die bereits eingeschaltet sind, werden weiterhin funktionieren, bis sie ausgeschaltet werden, da ihre Verbindungen zum Netzwerk bereits hergestellt sind.

Der optimale Ansatz besteht darin, ein Umbenennen der Netzwerke nach deren Verwendung zu vermeiden. Nach dem Umbenennen einer Port-Gruppe müssen Sie jede zugeordnete virtuelle Maschine, die die Servicekonsole verwendet, neu konfigurieren, um den neuen Port-Gruppennamen entsprechend zu berücksichtigen.

Speicher

Speicher - Einführung 5

Dieses Kapitel enthält eine Übersicht über die zur Verfügung stehenden Speicheroptionen für ESX Server.

Informationen über die Konfiguration von SANs finden Sie im *Handbuch der SAN-Konfiguration*.

In diesem Kapitel werden folgende Themen behandelt:

- „Speicherkonzepte“ auf Seite 88
- „Speicher - Übersicht“ auf Seite 89
- „Anzeige der Speicherinformationen im VI Client“ auf Seite 93
- „VMware Dateisystem“ auf Seite 97
- „Konfiguration und Verwaltung von Speicher“ auf Seite 101

Speicherkonzepte

Es sind bestimmte Grundlagen notwendig, um Speicher vollständig zu verstehen.

- **Datastore** – Formatierter logischer Datenbehälter analog einem Dateisystem auf einem logischen *Volume*. Der Datastore enthält die Dateien der virtuellen Maschinen. Er kann sich auf verschiedenen Typen von physischen Speichersystemen wie z. B. SCSI, iSCSI, Fibre-Channel-SAN oder NFS befinden. Es gibt zwei verschiedene Typen von Datastores: VMFS-basiert und NFS-basiert.
- **Festplattenpartition** – Ein für einen bestimmten Zweck abgegrenzter Teil einer Festplatte. Im Kontext des Speichers von ESX Server können Festplattenpartitionen auf verschiedenen physischen Speichergeräten reserviert und als Datastores formatiert werden.
- **Erweiterung** – Im Kontext ESX Server ist eine Erweiterung eine Festplattenpartition auf einem physischen Speichergerät, die dynamisch zu einem bestehenden Datastore im VMFS-basierten Format hinzugefügt werden kann. Ein Datastore kann sich über mehrere Erweiterungen erstrecken, erscheint jedoch ebenso wie ein *Speicher aus mehreren Datenträgern* wie ein einziger Datenträger.
- **Failover-Pfad** – Ein redundanter physischer Pfad, den das ESX Server-System verwenden kann, wenn es mit dem Netzwerkspeicher kommuniziert. Das ESX Server-System verwendet den Failover-Pfad, wenn eine Komponente, die für die Übertragung von Speicherdaten verantwortlich ist, ausfällt. Weitere Informationen finden Sie unter *„Multipathing“*.
- **Fibre-Channel (FC)** – Eine Hochgeschwindigkeitstechnologie für die Datenübertragung, die ESX Server-Systeme zum Übertragen von SCSI-Verkehr von virtuellen Maschinen auf Speichergeräte auf einem SAN verwenden. Das Fibre Channel Protocol (FCP) verpackt SCSI-Befehle in Fibre-Channel-Datenblöcke.
- **iSCSI (Internet-SCSI)** – Wandelt SCSI-Speicherdatenverkehr in TCP-Pakete um, sodass er über IP-Netzwerke statt über spezialisierte FC-Netzwerke übertragen werden kann. Mit einer iSCSI-Verbindung kommuniziert das ESX Server-System (Initiator) mit einem entfernten Speichergerät (Ziel), als wäre es eine lokale Festplatte.
- **LUN (Logical Unit Number, Logische Einheitennummer)** – Die Adresse, die jede SCSI-Festplatte eindeutig identifiziert, die von einem ESX Server-System als Speicher verwendet wird. Die Bezeichnungen *Festplatte* und *LUN* werden häufig untereinander austauschbar verwendet.
- **Multipathing** – Eine Technik, mit der Sie mehrere Pfade oder ein Element auf diesem Pfad zur Übertragung von Daten zwischen dem ESX Server-System und seinem fernen Speicher verwenden können. Diese redundante Verwendung von physischen Pfaden oder Elementen, wie z. B. Adaptern, ermöglicht ununterbrochenen Datenverkehr zwischen dem ESX Server-System und den Speichergeräten.

- **NAS (Network-Attached Storage, über das Netzwerk angebundener Speicher)** – Ein spezialisiertes Speichergerät, das an ein Netzwerk angeschlossen ist und Dateizugriff für ESX Server-Systeme bietet. ESX Server-Systeme verwenden das NFS-Protokoll, um mit NAS-Servern zu kommunizieren.
- **NFS (Network File System, Netzwerk-Dateisystem)** – Ein Dateiaustausch-protokoll, das ESX Server unterstützt, um mit NAS-Geräten zu kommunizieren.
- **Raw-Device (Raw-Festplatte)** – SCSI-Gerät, das von einer virtuellen Maschine direkt benutzt wird. Auf das Gerät kann mittels RDM-Zuordnung zugegriffen werden.
- **Raw Device Mapping (RDM)** – Eine spezielle Zuordnungsdatei in einem VMFS-Volume, die als Proxy für ein Raw-Device arbeitet und SAN-LUNs direkt einer virtuellen Maschine zuordnet. Die RDM-Datei kann auch als Metadatendatei bezeichnet werden.
- **Raw-LUN** – Logische Festplatte in einem SAN.
- **Datenträgerübergreifender Datenträger** – Ein dynamischer Datenträger, der Speicherplatz auf mehreren physischen Datenträgern belegt, aber als ein einziger logischer Datenträger erscheint.
- **Speichergerät** – Physische Festplatten- oder Speicherarrays, die sich entweder innerhalb oder außerhalb des Systems befinden können und an das System entweder direkt oder über einen Adapter angeschlossen sind.
- **VMFS (VMware File System, VMware Dateisystem)** – Hochleistungsfähiges Cluster-Dateisystem, das für virtuelle Maschinen optimierte Speicher-Virtualisierung bietet.
- **Datenträger** – Eine logische Speichereinheit, die Festplattenspeicher auf einem physischen Gerät, einem Teil davon oder übergreifend auf mehreren physischen Geräten verwendet.

Speicher - Übersicht

In den meisten Konfigurationen verwendet eine virtuelle Maschine eine virtuelle Festplatte, um das Betriebssystem, die Programmdateien und andere Daten für ihren Betrieb zu speichern. Eine virtuelle Festplatte ist eine große physische Datei, die sich so einfach wie jede andere Datei kopieren, verschieben, archivieren und sichern lässt.

Virtuelle Festplattendateien sind auf speziell formatierten Datenträgern gespeichert, die „Datastore“ genannt werden. Ein Datastore kann sich auf den internen, direkt angebundenen Speichergeräten des Hosts oder auf Netzwerkspeichergeräten befinden. Netzwerkspeichergeräte sind externe gemeinsam genutzte Speichergeräte oder Speicherarrays, die sich außerhalb des Systems befinden und auf die mithilfe eines Adapters über ein Netzwerk zugegriffen wird.

Das Speichern virtueller Festplatten und anderer wichtiger Bestandteile der virtuellen Maschinen in einem einzigen Datastore, der von mehreren physischen Hosts gemeinsam genutzt wird, ermöglicht:

- Die Verwendung von Funktionen wie VMware DRS (Distributed Resource Scheduling, verteilte Ressourcenplanung) und VMware HA (High Availability Options, Optionen für hohe Verfügbarkeit).
- Die Verwendung von VMotion für das Verschieben von aktiven virtuellen Maschinen von einem ESX Server auf einen anderen ohne Unterbrechung des Betriebs.
- Die Verwendung von Consolidated Backup, um Backups effizienter durchzuführen.
- Besseren Schutz vor geplanten oder ungeplanten Serverausfällen.
- Bessere Steuerung des Lastenausgleichs.

Mit ESX Server können Sie auf viele verschiedene - interne und externe - physische Speichergeräte zugreifen, die Sie auch konfigurieren und formatieren und für Ihre Speicherbedürfnisse verwenden können.

In dem meisten Fällen verwenden Sie zur Arbeit mit dem Speicher VI Client. Die folgenden Kapitel enthalten Informationen zum Zugriff und zur Konfiguration der Speichergeräte sowie zum Einsatz und zur Verwaltung von Datastores.

- „Speicherkonfiguration“ auf Seite 103
- „Speicherverwaltung“ auf Seite 137

Der verbleibende Teil des Abschnitts „Speicherübersicht“ befasst sich mit den folgenden Themen:

- „Datastores und Dateisysteme“ auf Seite 90
- „Dateisystemformate“ auf Seite 91
- „Speichertypen“ auf Seite 91
- „Unterstützte Speicheradapter“ auf Seite 92
- „Speicherzugriff durch virtuelle Maschinen“ auf Seite 92

Datastores und Dateisysteme

Die virtuellen Maschinen von ESX Server speichern ihre virtuellen Festplattendateien auf speziell formatierten logischen Datenbehältern, die sich auf verschiedenen Arten von physischen Speichergeräten befinden können. Ein Datastore kann dazu Festplattenplatz auf einem oder auf mehreren physischen Geräten verwenden.

Die Verwaltung des Datastores beginnt mit dem Speicherplatz, den die Speicherverwaltung für das ESX Server-System auf verschiedenen Speichergeräten zuweist. Der Speicherplatz wird dem ESX Server-System als LUNs oder, bei Netzwerkspeichern, als NFS-Datenträger dargestellt.

Mit dem VI Client können Sie Datastores erstellen, indem Sie auf die verfügbaren LUNs zugreifen und sie formatieren oder indem Sie die NFS-Datenträger einbinden.

Nach der Erstellung von Datastores können Sie diese dazu verwenden, VM-Dateien zu speichern. Gegebenenfalls können Sie die Datastores auch ändern. So können Sie zum Beispiel Erweiterungen für den Datastore hinzufügen oder Datastores umbenennen oder löschen.

Weitere Informationen zur Verwaltung von Datastores finden Sie unter „Verwaltung von Datastores und Dateisystemen“ auf Seite 138.

Dateisystemformate

Für Datastores stehen Ihnen folgende Dateisystemformate zur Verfügung:

- **VMFS** – ESX Server setzt diese Art Dateisystem auf lokalen SCSI-Festplatten, iSCSI-LUNs oder Fibre-Channel-LUNs ein und erstellt für jede virtuelle Maschine ein Verzeichnis. VMFS ist ein Cluster-Dateisystem, auf das mehrere ESX Server-Systeme gleichzeitig zugreifen können.

HINWEIS ESX Server 3.0 unterstützt VMFS Version 3 (VMFS-3). VMFS-3 ist nicht mit ESX Server-Versionen vor ESX Server 3.0 rückwärtskompatibel. Wenn Sie VMFS-2 verwenden, müssen Sie es auf VMFS-3 aktualisieren. Weitere Informationen zur Aktualisierung von VMFS-2 finden Sie unter „Aktualisierung von Datastores“ auf Seite 139.

Weitere Informationen zu VMFS finden Sie unter „VMware Dateisystem“ auf Seite 97.

Als Alternative zur Verwendung eines VMFS-basierten Datastores kann Ihre virtuelle Maschine, über einer Zuordnungsdatei (RDM) als Proxy, direkt auf Raw-Devices zugreifen. Weitere Informationen über RDM-Zuordnungen finden Sie unter „Raw-Device-Mapping“ auf Seite 151.

- **NFS** – ESX Server kann einen designierten NFS-Datenträger auf einem NFS-Server verwenden. ESX Server bindet den NFS-Datenträger ein und erstellt für jede virtuelle Maschine ein Verzeichnis. Aus der Sicht des Benutzers an einem Client-Rechner sind die aktivierten Dateien von lokalen Dateien nicht zu unterscheiden.

Speichertypen

Datastores können sich auf verschiedenen Speichergeräten befinden. Sie können einen Datastore auf einem direkt an das System angebundenen Speichergerät oder auf einem Netzwerkspeichergerät implementieren.

ESX Server unterstützt folgende Typen von Speichergeräten:

- **Lokal** – Speichert Dateien lokal auf einem internen oder externen SCSI-Gerät.

- **Fibre-Channel** – Speichert Dateien extern in einem Speichernetzwerk (Storage Area Network, SAN). Erfordert Fibre-Channel-Adapter.
- **iSCSI (hardware-initiiert)** – Speichert Dateien auf externen iSCSI-Speichergeräten. Auf die Dateien wird unter Verwendung eines hardware-basierten iSCSI-HBAs (Host-Bus-Adapter) über ein TCP/IP-Netzwerk zugegriffen.
- **iSCSI (software-initiiert)** – Speichert Dateien auf externen iSCSI-Speichergeräten. Auf die Dateien wird über ein TCP/IP-Netzwerk unter Verwendung von software-basiertem iSCSI-Code im VMkernel zugegriffen. Erfordert einen Standardnetzwerkadapter für die Netzwerkanbindung.
- **Netzwerk-Dateisystem (Network File System, NFS)** – Speichert Dateien auf externen Dateiservern. Auf die Dateien wird unter Verwendung des NFS-Protokolls über ein TCP/IP-Netzwerk zugegriffen. Erfordert einen Standardnetzwerkadapter für die Netzwerkanbindung.

HINWEIS Sie können virtuelle Maschinen auf IDE- oder SATA-Laufwerken speichern. Der ESX Server-Host muss über einen SCSI-Speicher, einen NAS oder ein SAN zum Speichern virtueller Maschinen verfügen.

Mit dem VI Client greifen Sie auf die Speichergeräte zu, die dem ESX Server-System zugewiesen wurden, und implementieren darauf Datastores. Weitere Informationen finden Sie unter „Speicherkonfiguration“ auf Seite 103.

Unterstützte Speicheradapter

Für den Zugriff auf verschiedene Speichertypen benötigt das ESX Server-System verschiedene Adapter, um eine Verbindung zum Speichergerät oder zum Netzwerk aufbauen zu können. ESX Server unterstützt PCI-basierte SCSI- und iSCSI-, RAID-, Fibre-Channel- und Ethernet-Adapter und greift direkt über die Gerätetreiber im VMkernel darauf zu.

Speicherzugriff durch virtuelle Maschinen

Wenn eine virtuelle Maschine mit virtuellen Festplatten kommuniziert, die auf einem Datastore gespeichert sind, gibt sie SCSI-Befehle aus. Da sich die Datastores auf verschiedenen Typen von physischen Speichern befinden können, werden diese Befehle je nach Protokoll, dass das ESX Server-System zur Anbindung an ein Speichergerät verwendet, umgewandelt. ESX Server unterstützt die Protokoll Fibre-Channel (FC), Internet-SCSI (iSCSI) und NFS.

Die Abbildung Abbildung 5-1 zeigt die Unterschiede zwischen den Speichertypen: Fünf virtuelle Maschinen verwenden unterschiedliche Typen von Speichern.

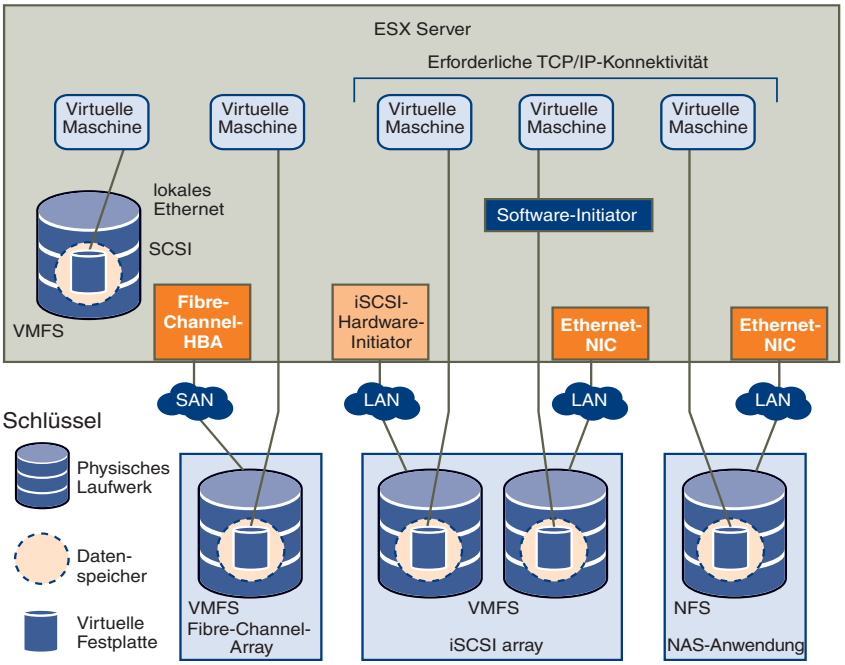


Abbildung 5-1. Speichertypen

HINWEIS Diese Abbildung dient nur zur Veranschaulichung. Es handelt sich dabei nicht um eine empfohlene Konfiguration.

Sie können eine virtuelle Maschine so konfigurieren, dass sie auf die virtuellen Festplatten auf den physischen Speichergeräten zugreifen kann. Weitere Informationen zur Konfiguration von virtuellen Maschinen finden Sie im *Handbuch zur Verwaltung von virtuellen Maschinen*.

Anzeige der Speicherinformationen im VI Client

Der VI Client zeigt detaillierte Informationen über verfügbare Datastores, Speichergeräte, die von den Datastores verwendet werden, und über die Adapterkonfiguration an. Weitere Informationen finden Sie in folgenden Abschnitten:

- „Anzeige von Datastores“ auf Seite 94
- „Anzeige der Speicheradapter“ auf Seite 95
- „Grundlegendes zur Benennung von Speichergeräten in der Anzeige“ auf Seite 96

Anzeige von Datastores

Es gibt zwei Möglichkeiten, dem VI Client Datastores hinzufügen:

- Erkennung beim Hinzufügen eines Hosts zum Inventar – Wenn Sie der Inventar einen Host hinzufügen, zeigt VI Client alle Datastores an, die der Host erkennt.
- Erstellung auf einem verfügbaren Speichergerät – Mithilfe der Option **Speicher hinzufügen** können Sie einen neuen Datastore erstellen und konfigurieren. Weitere Informationen finden Sie unter „Speicherkonfiguration“ auf Seite 103.

Sie können ein Verzeichnis der verfügbaren Datastores anzeigen lassen und ihre Eigenschaften analysieren.

Um Datastores anzuzeigen, klicken Sie auf der Registerkarte „Konfiguration“ des Hosts auf den Link **Speicher (SCSI, SAN und NFS)**.

Der Speicherabschnitt zeigt für jeden Datastore eine Übersicht an. Hier sind folgende Daten zu finden:

- Zielspeichergerät, auf dem sich der Datastore befindet. Siehe „Grundlegendes zur Benennung von Speichergeräten in der Anzeige“ auf Seite 96.
- Dateisystem, das der Datastore verwendet. Weitere Informationen finden Sie unter „Dateisystemformate“ auf Seite 91.
- Gesamtkapazität sowie verwendeter und freier Speicher.

Wählen Sie den Datastore aus dem Verzeichnis aus, wenn Sie zusätzlich Details zu dem Datastore erfahren möchten. Der Details-Abschnitt enthält folgende Daten:

- Speicherort des Datastores.
- Einzelne Erweiterungen, die der Datastore belegt, und deren Kapazität.
- Pfade, die zum Zugriff auf das Speichergerät verwendet werden.

In Abbildung 5-2 wurde der Datastore „symm-07“ aus der Liste der verfügbaren Datastores ausgewählt. Die **Detailansicht** zeigt Informationen zum ausgewählten Datastore an.

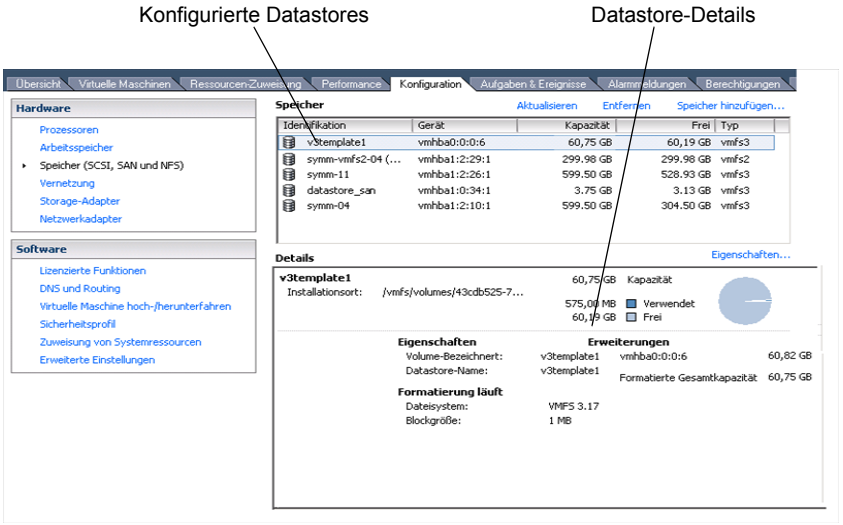


Abbildung 5-2. Informationen zu Datastores

Sie können alle bestehenden Datastores bearbeiten und verschieben. Bei der Bearbeitung eines Datastores können Sie seine Bezeichnung ändern, Erweiterungen hinzufügen oder Pfade zu den Speichergeräten ändern. Sie können den Datastore auch aktualisieren. Weitere Informationen finden Sie unter „Speicherverwaltung“ auf Seite 137.

Anzeige der Speicheradapter

Der VI Client zeigt alle Speicheradapter an, die im System zur Verfügung stehen.

Um Speicheradapter anzuzeigen, klicken Sie auf der Registerkarte **Konfiguration** des Hosts auf den Link **Speicheradapter**.

Sie können sich über Speicheradapter die folgenden Informationen anzeigen lassen:

- Bestehende Speicheradapter.
- Art des Speicheradapters, z. B. Fibre Channel, SCSI oder iSCSI.
- Details zu jedem Adapter, wie z. B. das angebundene Speichergerät und die Target-ID.

Um die Konfigurationseigenschaften eines bestimmten Adapters anzuzeigen, markieren Sie den Adapter in der Liste **Speicheradapter**.

In Abbildung 5-3 wurde der Fibre-Channel-Speicheradapter „vmhba0“ markiert. Die **Detailansicht** gibt Auskunft über die Anzahl der LUNs, an die der Adapter angebunden ist, und über die verwendeten Pfade.

Wenn Sie die Konfiguration des Pfads ändern wollen, markieren Sie den Pfad in der Liste, klicken mit der rechten Maustaste auf den Pfad und klicken auf **Pfade verwalten**. Der Assistent **Pfade verwalten** wird geöffnet. Weitere Informationen zur Verwaltung von Pfaden finden Sie unter „Verwalten von Pfaden für Fibre-Channel und iSCSI“ auf Seite 143.

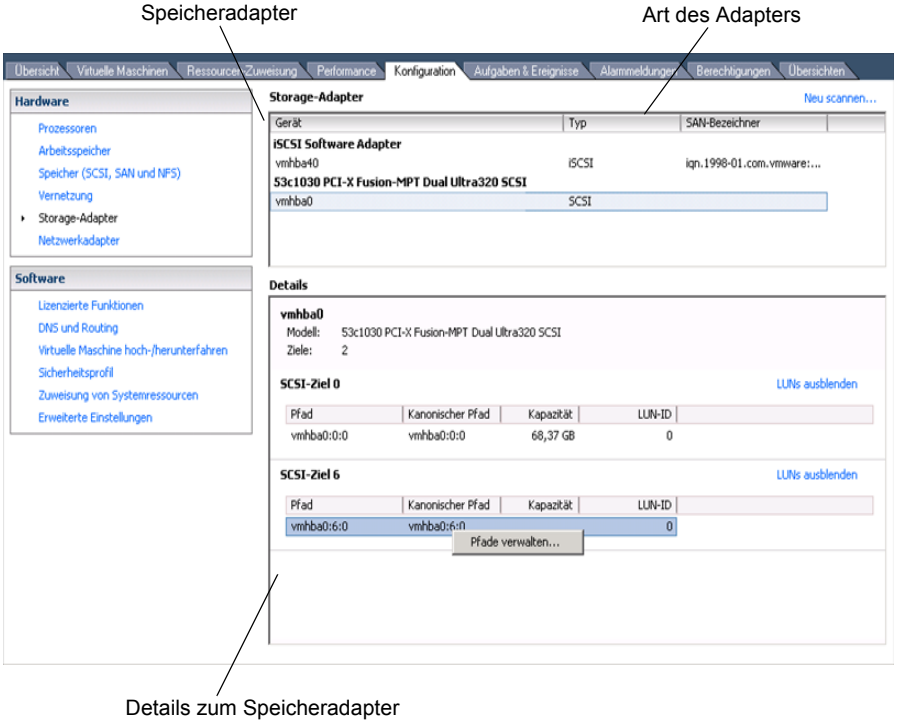


Abbildung 5-3. Informationen zu Speicheradaptern

Grundlegendes zur Benennung von Speichergeräten in der Anzeige

In VI Client wird der Name eines Speichergeräts als Abfolge von drei oder vier Zahlen angegeben, die durch Doppelpunkte getrennt sind, z. B. `vmhba1:1:3:1`. Dieser Name hat die folgende Bedeutung:

```
<HBA>:<SCSI target>:<SCSI LUN>:<disk partition>
```

Die Abkürzung `vmhba` bezieht sich auf verschiedene physische HBAs im ESX Server-System. Sie kann sich auch auf den virtuellen iSCSI-Initiator beziehen, den ESX Server unter Verwendung des VMkernel-Netzwerk-Stacks implementiert. Die vierte Zahl gibt eine Partition auf einer Festplatte oder einer LUN an. Wenn ein Datastore die gesamte Festplatte oder LUN belegt, fehlt die vierte Zahl.

Das Beispiel `vmhba1:1:3:1` bezieht sich auf die erste Partition auf SCSI-LUN 3, SCSI-Ziel 1, auf die durch HBA 1 zugegriffen wird.

Die dritte und vierte Zahl ändern sich nie, die ersten beiden Zahlen können sich jedoch ändern. Beispielsweise kann sich nach einem Neustart des ESX Server-Systems `vmhba1:1:3:1` zu `vmhba3:2:3:1` ändern; der Name bezieht sich jedoch immer noch auf dasselbe physische Gerät. Die erste und zweite Zahl können sich aus den folgenden Gründen ändern:

- Die erste Zahl, der HBA, ändert sich, wenn auf dem Fibre-Channel- oder iSCSI-Netzwerk ein Ausfall auftritt. In diesem Fall muss das ESX Server-System für den Zugriff auf das Speichergerät einen anderen HBA verwenden.
- Die zweite Zahl, das SCSI-Ziel, ändert sich im Falle von Modifizierungen bei der Zuordnung der Fibre-Channel- oder iSCSI-Ziele, die für den ESX Server-Host sichtbar sind.

VMware Dateisystem

Ein Dateisystem ist ein Verfahren für das Speichern, Organisieren, Zugreifen auf, Navigieren durch und Auslesen von Computerdateien und der in ihnen enthaltenen Daten. Dateisysteme können unterschiedliche Formate aufweisen, wie z. B. FAT, NTFS, HPFS, UFS und EXT3. VMware bietet ein spezielles Hochleistungsdateisystem mit der Bezeichnung VMware File System (VMFS), das für die Speicherung virtueller ESX Server-Maschinen optimiert wurde.

In diesem Abschnitt sind Informationen über VMFS sowie folgende Themen enthalten:

- „VMFS-Versionen“ auf Seite 97
- „Erstellen und Vergrößern eines VMFS“ auf Seite 98
- „VMFS-Funktionen für den gemeinsamen Zugriff“ auf Seite 99

VMFS-Versionen

ESX Server bietet die folgenden Versionen dieses Dateisystems:

- **VMFS2** – Dieses Dateisystem wird mit ESX Server Version 2.x erstellt.
- **VMFS3** – Dieses Dateisystem wurde mit ESX Server der Version3 erstellt. Zu den Verbesserungen von VMFS3 gehört die Unterstützung mehrerer Verzeichnisse. Eine virtuelle Maschine muss auf einem VMFS3-Dateisystem eingerichtet sein, bevor ein Host mit ESX Server Version 3 sie einschalten kann.

Tabelle 5-1. Host-Zugriff auf VMFS-Dateisysteme

Host	VMFS2-Datastore	VMFS3-Datastore
Host mit ESX Server Version 2	Lesen/Schreiben (führt VMs aus)	Kein Zugriff
Host mit ESX Server Version 3	Nur lesen (kopiert VMs)	Lesen/Schreiben (führt VMs aus)

Erstellen und Vergrößern eines VMFS

VMFS lässt sich auf einer Reihe von SCSI-basierten Speichergeräten einsetzen, einschließlich Fibre-Channel- und iSCSI-SAN-Systemen. Eine unter VMFS gespeicherte virtuelle Festplatte erscheint der virtuellen Maschine immer als aktiviertes SCSI-Gerät. Die virtuelle Festplatte verbirgt eine physische Speicherschicht vor dem Betriebssystem der virtuellen Maschine. Daher können Sie in der virtuellen Maschine selbst Betriebssysteme ausführen, die nicht für SAN zertifiziert sind.

Für das Betriebssystem innerhalb der virtuellen Maschine behält VMFS die interne Dateisystem-Semantik bei. Dadurch werden das ordnungsgemäße Verhalten von Anwendungen und die Datensicherheit für Anwendungen gewährleistet, die in virtuellen Maschinen ausgeführt werden.

Sie können VMFS-basierte Datastores im Voraus auf jedem Speichergerät einrichten, das Ihr ESX Server erkennt. Wählen Sie eine hohe LUN, wenn Sie die Absicht haben, darauf mehrere virtuelle Maschinen einzurichten. Sie können dann virtuelle Maschinen dynamisch hinzufügen, ohne zusätzliche Festplattenkapazität anfordern zu müssen.

Falls jedoch mehr Platz benötigt wird, können Sie das VMFS-Volume jederzeit vergrößern – auf bis zu 64 TB.

Informationen darüber, was bei der Erstellung eines VMFS besonders zu beachten ist, finden Sie unter „Überlegungen beim Erstellen von VMFS“ auf Seite 98.

Überlegungen beim Erstellen von VMFS

Bevor Sie Speichergeräte mit VMFS formatieren, müssen Sie zunächst festlegen, wie Sie den Speicher für Ihre ESX Server-Systeme einrichten wollen. Sie sollten immer nur ein VMFS-Volume pro LUN haben. Allerdings können Sie entweder ein großes VMFS-Volume oder mehrere kleine einsetzen. Mit ESX Server können Sie bis zu 256 VMFS-Volumes pro System verwenden, die Volume-Mindestgröße beträgt dabei jeweils 1,2 GB.

Die folgenden Gründe sprechen für weniger und dafür größere VMFS-Volumes:

- Mehr Flexibilität beim Erstellen virtueller Maschinen, ohne beim Speicher-Administrator mehr Platz anfordern zu müssen.
- Mehr Flexibilität bei der Größenänderung virtueller Festplatten, dem Erstellen von Snapshots usw.
- Weniger zu verwaltende VMFS-basierte Datastores.

Die folgenden Gründe sprechen für mehr und dafür kleinere VMFS-Volumes:

- Weniger Konkurrenzsituationen auf den einzelnen VMFS aufgrund von Sperren und SCSI-Reservierungen.
- Weniger verschwendeter Speicherplatz.
- Unterschiedliche Anwendungen könnten unterschiedliche RAID-Charakteristiken erfordern.
- Mehr Flexibilität, da die Multipathing-Richtlinie und gemeinsam genutzte Festplattenbereiche pro LUN festgelegt werden.
- Für den Einsatz von Microsoft Cluster Service muss jede Cluster-Festplatten-Ressource in ihrer eigenen LUN eingerichtet sein.

Unter Umständen könnte es sinnvoll sein, einige Ihrer Server für wenige, größere VMFS-Volumes zu konfigurieren und andere für mehr und kleinere VMFS-Volumes.

VMFS-Funktionen für den gemeinsamen Zugriff

Sie können mehrere virtuelle Maschinen auf einem einzigen VMFS-Volume speichern und mehreren ESX Servern den Zugriff darauf gewähren.

Weitere Informationen finden Sie in folgenden Abschnitten:

- „Speichern mehrerer virtueller Maschinen auf einem VMFS-Volume“ auf Seite 99
- „Gemeinsames Nutzen eines VMFS-Volumes durch mehrere ESX Server“ auf Seite 100

Speichern mehrerer virtueller Maschinen auf einem VMFS-Volume

Sie können mehrere virtuelle Maschinen auf demselben VMFS-Volume speichern. Jede virtuelle Maschine ist in einem kleinen Satz Dateien eingekapselt und belegt ein eigenes Verzeichnis. VMFS unterstützt die folgenden Datei- und Blockgrößen, sodass Sie auch die datenhungrigsten Anwendungen wie Datenbanken, ERP und CRM in virtuellen Maschinen ausführen können:

- Maximale Größe der virtuellen Festplatte: 2 TB
- Maximale Dateigröße: 2 TB
- Blockgröße: 1 MB bis 8 MB

Wenn Sie vorhaben, mehrere virtuelle Maschinen auf demselben VMFS-Volume zu speichern, berücksichtigen Sie den folgenden Grundsatz: Je mehr virtuelle Maschinen sich dasselbe Volume teilen, desto größer ist die potenzielle Leistungsverschlechterung als Folge von I/O-Konkurrenzsituationen.

Gemeinsames Nutzen eines VMFS-Volumes durch mehrere ESX Server

Als Cluster-Dateisystem ermöglicht es VMFS mehreren ESX Servern, parallel auf dasselbe Speichermedium zuzugreifen. Sie können bis zu 32 ESX Server mit einem einzigen VMFS-Volume verbinden.

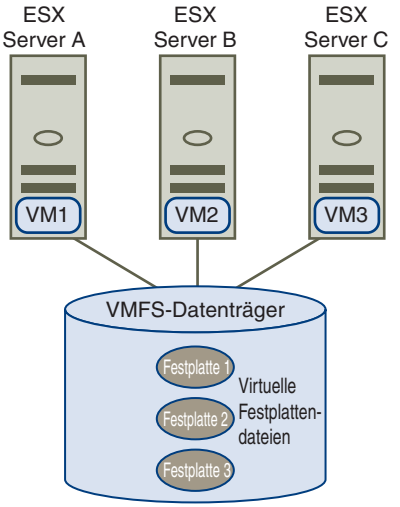


Abbildung 5-4. Gemeinsames Nutzen eines VMFS-Volumes durch mehrere ESX Server

Um zu gewährleisten, dass nicht mehrere Server gleichzeitig auf dieselbe virtuelle Maschine zugreifen, verfügt VMFS über eine platteninterne Sperrung.

Die gemeinsame Nutzung desselben VMFS-Volumes durch mehrere ESX Server bietet Ihnen die folgenden Vorteile:

- Sie können virtuelle Maschinen über mehrere physische Server hinweg verteilen. Das bedeutet: Sie führen auf jedem Server einen Mix virtueller Maschinen aus, sodass nicht alle zur selben Zeit im selben Bereich einer hohen Nachfrage unterliegen.
- Falls ein Server ausfällt, können Sie die virtuellen Maschinen auf einem anderen physischen Server neu starten. Im Störfall wird die platteninterne Sperre für die einzelnen virtuellen Maschinen aufgehoben.
- Mit VMotion können Sie Live-Migrationen von virtuellen Maschinen während des laufenden Betriebs von einem physischen Server zu einem anderen durchführen.
- Mit Consolidated Backup kann ein Proxy-Server einen Snapshot einer virtuellen Maschine sichern, während diese eingeschaltet wird und in ihren Speicher schreibt und daraus liest.

Konfiguration und Verwaltung von Speicher

Die Kapitel „Konfigurieren des Speichers“ und „Verwalten des Speichers“ in diesem Handbuch enthalten die wichtigsten Konzepte und Aufgaben, die bei der Arbeit mit Speicher erforderlich sind.

Detaillierte Informationen zur Konfiguration von SANs finden Sie im *Handbuch der SAN-Konfiguration*.

In den folgenden Abschnitten sind die Speicheraufgaben erläutert, die Sie in ESX Server durchführen können.

Lokale SCSI-Konfigurationsaufgaben

„Erstellung eines Datastores auf einer lokalen SCSI-Festplatte“ auf Seite 105

Fibre-Channel-Aufgaben

„Erstellung eines Datastores auf einem Fibre-Channel-Gerät“ auf Seite 108

Hardware-initiierte iSCSI-Aufgaben

- „Anzeige der Eigenschaften des iSCSI-Hardware-Initiators“ auf Seite 114
- „So richten Sie den iSCSI-Namen und die IP-Adresse für den Hardware-Initiator ein.“ auf Seite 116
- „Einrichtung von Zielerkennungsadressen für den Hardware-Initiator“ auf Seite 117
- „Einrichtung der CHAP-Parameter für den Hardware-Initiator“ auf Seite 119
- „Erstellung eines Datastores auf einem hardware-initiierten iSCSI-Gerät“ auf Seite 120

Software-initiierte iSCSI-Aufgaben

- „Anzeige der Eigenschaften des iSCSI-Software-Initiators“ auf Seite 122
- „Aktivierung des iSCSI-Software-Initiators“ auf Seite 125
- „So richten Sie Zielerkennungsadressen für den Software-Initiator ein:“ auf Seite 126
- „Einrichtung der CHAP-Parameter für den Software-Initiator“ auf Seite 128
- „Erstellung eines Datastores auf einem software-initiierten iSCSI-Gerät“ auf Seite 129

NFS-Aufgaben

„Einbindung eines NFS-Datenträgers“ auf Seite 135

Allgemeine Speicheraufgaben

- „Aktualisierung von VMFS-2 in VMFS-3“ auf Seite 140
- „Bearbeiten des Datastore-Namens“ auf Seite 140
- „Hinzufügen von Erweiterungen zu einem Datastore“ auf Seite 141
- „Entfernen eines Datastores“ auf Seite 139

Pfadverwaltungsaufgaben

- „So richten Sie die Multipathing-Policy ein“ auf Seite 147
- „So deaktivieren Sie einen Pfad“ auf Seite 149
- „So richten Sie den bevorzugten Pfad ein“ auf Seite 150

Speicherkonfiguration 6

Dieses Kapitel enthält Informationen zur Konfiguration lokaler SCSI-Festplatten, zum Speichern in Fibre-Channel-Speichernetzwerken (FC-SANs), zum Speichern mit iSCSI und zu NFS-Volumes.

HINWEIS Zusätzliche Informationen zur Konfiguration von SANs finden Sie im *Handbuch zur SAN-Konfiguration*.

In diesem Kapitel werden folgende Themen behandelt:

- „Lokaler SCSI-Festplattenspeicher“ auf Seite 104
- „Fibre-Channel-Speicher“ auf Seite 106
- „iSCSI-Speicher“ auf Seite 110
- „NAS-Netzwerkspeicher“ auf Seite 132

Lokaler SCSI-Festplattenspeicher

Die einfachsten Speicher verwenden ein SCSI-Gerät wie z. B. die Festplatte des Systems oder ein externes SCSI-Speichergerät.

Die folgende Abbildung Abbildung 6-1 zeigt eine virtuelle Maschine, die einen lokalen SCSI-Speicher verwendet.

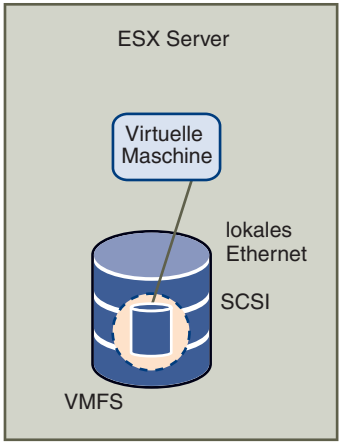


Abbildung 6-1. Lokaler SCSI-Speicher

In diesem Beispiel einer lokalen Speicherkonfiguration wird die ESX Server-SCSI-Karte über ein Kabel an die Festplatte angeschlossen. Auf dieser Festplatte können Sie einen Datastore erstellen, der zur Speicherung der Festplattendateien der virtuellen Maschine verwendet wird. Der Datastore, der erstellt wird, ist im VMFS-Format.

Weitere Informationen zum Konfigurieren des lokalen Speichers auf internen oder externen SCSI-Geräten finden Sie unter „Hinzufügen von lokalem SCSI-Speicher“ auf Seite 104.

Hinzufügen von lokalem SCSI-Speicher

Beim Laden der Treiber für die SCSI-Speicheradapter erkennt ESX Server die verfügbaren SCSI-Speichergeräte. Bevor Sie einen neuen Datastore auf einem SCSI-Gerät durchführen, müssen Sie ggf. neu nach Speichergeräten scannen. Weitere Informationen finden Sie unter „Neu scannen“ auf Seite 131.

Wenn Sie einen Datastore auf einem SCSI-Speicher-Device erstellen, führt Sie der **Assistent zum Hinzufügen von Speicher** durch die Konfiguration.

Erstellung eines Datastores auf einer lokalen SCSI-Festplatte

1 Melden Sie sich am VMware VI Client an und wählen Sie den Server aus dem Inventar aus.

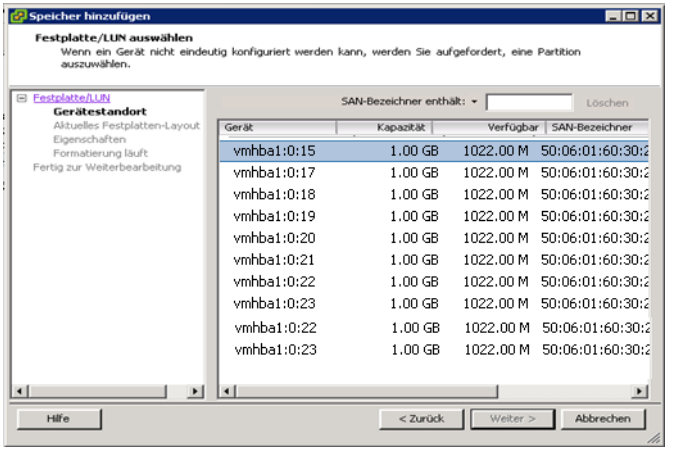
2 Klicken Sie auf die Registerkarte **Konfiguration** und klicken Sie unter Hardware auf **Speicher (SCSI, SAN und NFS)**.

3 Klicken Sie auf **Speicher hinzufügen**.

Das Dialogfeld **Speichertyp auswählen** wird angezeigt.

4 Markieren Sie den Speichertyp **Disk/LUN** (Festplatte/LUN) und klicken Sie auf **Weiter**.

Das Dialogfeld **„Disk/LUN** (Festplatte/LUN)**“** wird angezeigt.



5 Wählen Sie das SCSI-Gerät aus, das Sie für den Datastore verwenden möchten, und klicken Sie auf **Weiter**.

Das **Aktuelle Festplatten-Layout** wird angezeigt.

6 Überprüfen Sie das aktuelle Festplatten-Layout und klicken Sie auf **Weiter**.

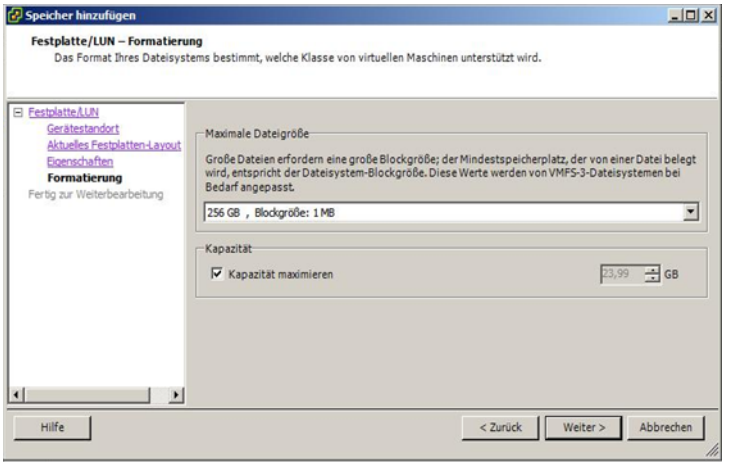
Das Dialogfeld **Festplatte/LUN–Eigenschaften** wird angezeigt.

7 Geben Sie einen Namen für den Datastore ein.

Der Name muss in der vorliegenden Instanz der virtuellen Infrastruktur eindeutig sein.

8 Klicken Sie auf **Weiter**.

Das Dialogfeld **Festplatte/LUN–Formatierung** wird angezeigt.



9 Passen Sie bei Bedarf das Dateisystem und die Größen an.

Standardmäßig wird der gesamte freie Speicherplatz des Speichergerätes angeboten.

10 Klicken Sie auf **Weiter**.

Das Dialogfeld **Fertig zur Weiterbearbeitung** wird angezeigt.

11 Überprüfen Sie die Konfigurationsdaten für den Datastore und klicken Sie auf **Fertig stellen**.

Durch diesen Prozess wird ein Datastore auf einer lokalen SCSI-Festplatte auf Ihrem ESX Server-Host erstellt.

Fibre-Channel-Speicher

ESX Server unterstützt Fibre-Channel-Adapter, über die ein ESX Server-System an ein SAN angebunden werden kann und das somit in der Lage ist, die Festplatten-Arrays im SAN zu erkennen.

Die Abbildung Abbildung 6-2 zeigt virtuelle Maschinen, die einen Fibre-Channel-Speicher verwenden.

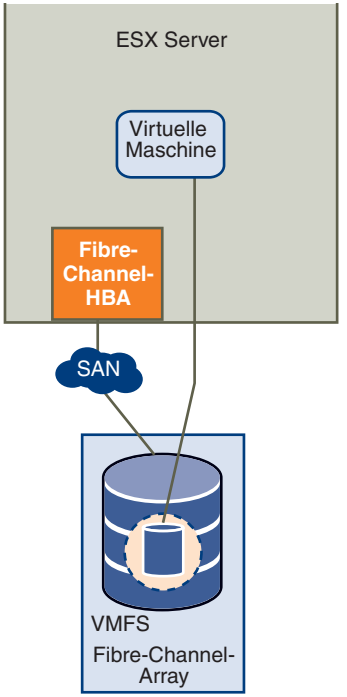


Abbildung 6-2. Fibre-Channel-Speicher

In dieser Konfiguration ist das ESX Server-System mithilfe eines Fibre-Channel-Adapters mit einem SAN-Fabric verbunden, das aus Fibre-Channel-Switches und Speicher-Arrays besteht. LUNs des Speicher-Arrays können nun vom ESX Server-System verwendet werden. Sie können auf die LUNs zugreifen und einen Datastore erstellen, der für die Speicheranforderungen von ESX Server verwendet werden kann. Der Datastore verwendet das VMFS-Format.

Informationen über das Konfigurieren des Fibre-Channel-Speichers finden Sie unter „Hinzufügen von Fibre-Channel-Speicher“ auf Seite 108.

In den folgenden Dokumenten erhalten Sie zusätzliche Informationen:

- Informationen über die Konfiguration von SANs finden Sie im *Handbuch zur SAN-Konfiguration*.
- Informationen über unterstützte SAN-Speicher-Device für ESX Server finden Sie im *Handbuch der SAN-Kompatibilität*.
- Informationen über Multipathing für Fibre-Channel-HBAs und die Verwaltung dieser Pfade finden Sie unter „Verwalten von Pfaden für Fibre-Channel und iSCSI“ auf Seite 143.

Hinzufügen von Fibre-Channel-Speicher

Scannen Sie den Fibre-Channel-Adapter vor der Erstellung eines neuen Datastores, um neu hinzugefügte LUNs zu erkennen. Weitere Informationen finden Sie unter „Neu scannen“ auf Seite 131.

Wenn Sie einen Datastore auf einem Fibre-Channel-Speicher-Device erstellen, führt Sie der **Assistent zum Hinzufügen von Speicher** durch die Konfiguration.

Erstellung eines Datastores auf einem Fibre-Channel-Gerät

1 Melden Sie sich am VMware VI Client an und wählen Sie einen Server aus dem Inventar aus.

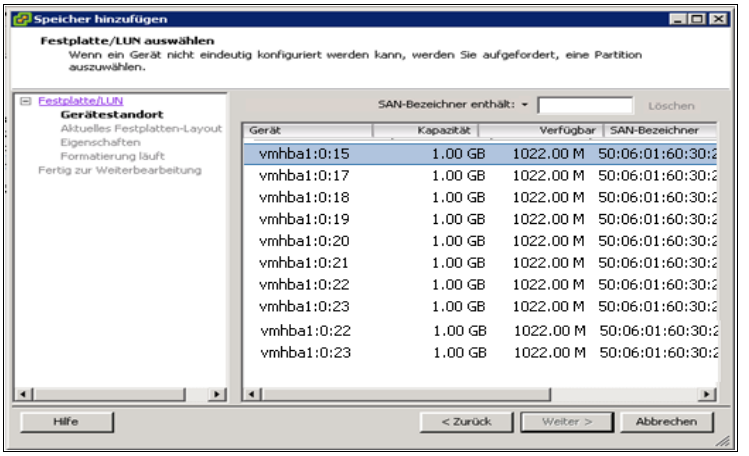
2 Klicken Sie auf die Registerkarte **Konfiguration** und klicken Sie unter Hardware auf **Speicher (SCSI, SAN und NFS)**.

3 Klicken Sie auf **Speicher hinzufügen**.

Das Dialogfeld **Speichertyp auswählen** wird angezeigt.

4 Markieren Sie den Speichertyp **Disk/LUN** (Festplatte/LUN) und klicken Sie auf **Weiter**.

Das Dialogfeld **„Disk/LUN** (Festplatte/LUN)“ wird angezeigt.



5 Wählen Sie das Fibre-Channel-Gerät aus, das Sie für den Datastore verwenden möchten, und klicken Sie auf **Weiter**.

Das **aktuelle Festplatten-Layout** wird angezeigt.

6 Überprüfen Sie das aktuelle Festplatten-Layout und klicken Sie auf **Weiter**.

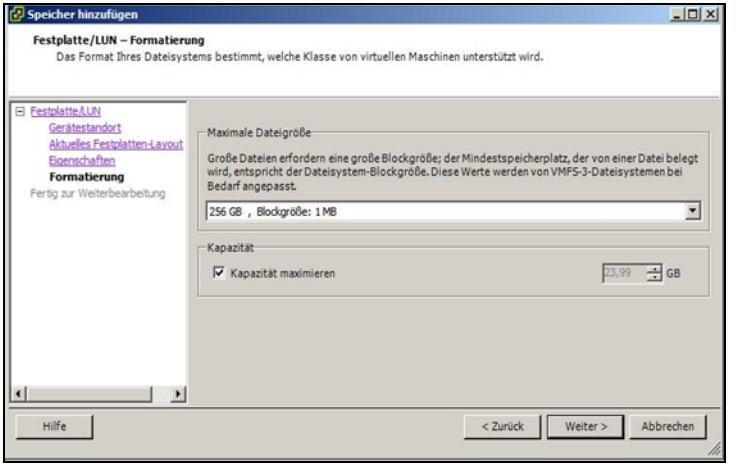
Das Dialogfeld **Festplatte/LUN–Eigenschaften** wird angezeigt.

7 Geben Sie einen Namen für den Datastore ein.

Der Name des Datastores wird im VI Client angezeigt und muss in der vorliegenden Instanz der virtuellen Infrastruktur eindeutig sein.

8 Klicken Sie auf **Weiter**.

Das Dialogfeld **Festplatte/LUN–Formatierung** wird angezeigt.



9 Ändern Sie bei Bedarf die Werte für das Dateisystem und die Größe des Datastores.

Standardmäßig wird der gesamte freie Speicherplatz des Speichergerätes angeboten.

10 Klicken Sie auf **Weiter**.

Das Dialogfeld **Fertig stellen** wird angezeigt.

11 Überprüfen Sie die Daten für den Datastore und klicken Sie auf **Fertig stellen**.

Dieser Prozess erstellt einen Datastore für den ESX Server-Host auf einer Fibre-Channel-Festplatte.

12 Scannen Sie nach neuen Speichergeräten.

Weitere Informationen finden Sie unter „Neu scannen“ auf Seite 131.

Informationen zur erweiterten Konfiguration, wie z. B. die Verwendung von Multipathing, Masking und Zoning finden Sie im *Handbuch zur SAN-Konfiguration*.

iSCSI-Speicher

Dieser Abschnitt enthält die folgenden Informationen zur Konfiguration von iSCSI-Speichern:

- „iSCSI-Speicher“ auf Seite 110
- „Konfigurieren von mittels Hardware ausgelöster iSCSI-Speicherung“ auf Seite 113
- „Konfiguration von software-initiiertem iSCSI-Speicher“ auf Seite 121

Weitere Informationen über Multipathing finden Sie unter „Verwalten von Pfaden für Fibre-Channel und iSCSI“ auf Seite 143.

iSCSI-Speicher

ESX Server 3.0 unterstützt die iSCSI-Technologie, die es dem ESX Server-System ermöglicht, beim Zugriff auf entfernten Speicher ein IP-Netzwerk zu verwenden. Bei iSCSI werden die SCSI-Speicherbefehle, die die virtuelle Maschine an ihre virtuelle Festplatte ausgibt, in TCP/IP-Protokoll-Pakete umgewandelt und an ein entferntes Gerät, das Ziel, übertragen, auf dem die virtuelle Festplatte gespeichert ist. Aus Sicht der virtuellen Maschine erscheint das Gerät als lokal angeschlossenes SCSI-Laufwerk.

Dieser Abschnitt enthält Informationen über iSCSI-Konzepte sowie folgende weitere Themen:

- „iSCSI Initiatoren“ auf Seite 110
- „Namenskonventionen“ auf Seite 112
- „Erkennung von Speicherressourcen“ auf Seite 112
- „iSCSI-Sicherheit“ auf Seite 113

iSCSI Initiatoren

Zum Zugriff auf entfernte Ziele verwendet der ESX Server-Host iSCSI-Initiatoren. Die Initiatoren transportieren SCSI-Anfragen und -Antworten zwischen dem ESX Server-System und dem Zielspeichergerät über das IP-Netzwerk.

ESX Server unterstützt hardware-basierte und software-basierte iSCSI-Initiatoren:

- **Hardware-iSCSI-Initiator** – Ein Drittanbieter-HBA mit der Funktion „iSCSI für TCP/IP“. Dieser spezialisierte iSCSI-Adapter ist für die gesamte Verarbeitung und das Management von iSCSI verantwortlich. Derzeit unterstützt ESX Server nur QLogic QLA4010 iSCSI HBA.
- **Software-iSCSI-Initiator** – Ein in den VMkernel integrierter Code, der es ermöglicht, das ESX Server-System mit dem iSCSI-Speicher-Device über Standardnetzwerkadapter anzubinden. Der Software-Initiator kümmert sich um die iSCSI-Verarbeitung und kommuniziert gleichzeitig über den Protokollstapel mit dem Netz-

werkadapter. Mit dem Software-Initiator können Sie die iSCSI-Technologie verwenden, ohne spezialisierte Hardware anschaffen zu müssen.

HINWEIS Die Gast-Betriebssysteme in den virtuellen Maschinen können den iSCSI-Speicher nicht direkt erkennen. Für die Gast-Betriebssysteme erscheint der an das ESX Server-System angebundene iSCSI-Speicher so, als wäre er über einen SCSI-HBA angebunden.

Die Abbildung Abbildung 6-3 zeigt zwei virtuelle Maschinen, die verschiedene Typen von iSCSI-Initiatoren verwenden.

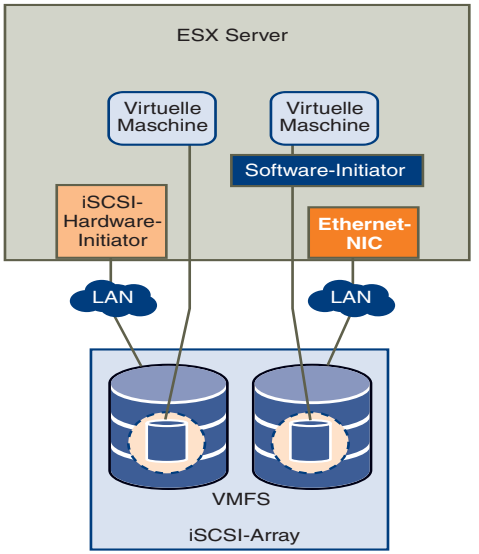


Abbildung 6-3. iSCSI-Speicher

Im ersten Beispiel der iSCSI-Speicherkonfiguration verwendet das ESX Server-System einen Hardware-iSCSI-Adapter. Dieser spezielle iSCSI-Adapter sendet iSCSI-Pakete über ein LAN an eine Festplatte.

Im zweiten Beispiel verfügt das ESX Server-System über einen Software-iSCSI-Initiator. Unter Verwendung des Software-Initiators stellt das ESX Server-System die Verbindung zu einem LAN über eine vorhandene Netzwerkkarte her.

HINWEIS Dieser Version von ESX Server unterstützt die gleichzeitige Verwendung von Hardware- und Software-iSCSI-Initiatoren auf dem gleichen ESX Server-System nicht. Verwenden Sie daher den Software-Initiator nur, wenn der iSCSI-Datenverkehr über einen normalen Netzwerkadapter abgewickelt wird, nicht jedoch, wenn spezielle iSCSI-Adapter verwendet werden.

Namenskonventionen

Da SANs sehr groß und komplex werden können, verfügen alle iSCSI-Initiatoren und -Ziele im Netzwerk über eindeutige und dauerhafte iSCSI-Namen. Außerdem werden ihnen Zugriffsadressen zugewiesen. Der iSCSI-Name ermöglicht die korrekte Identifizierung eines bestimmten iSCSI-Gerätes (Initiator oder Ziel), unabhängig davon, wo es sich befindet.

Stellen Sie bei der Konfiguration der iSCSI-Initiatoren sicher, dass die Namens- konventionen eingehalten werden. Die Initiatoren können folgende Formate verwenden:

- **IQN (iSCSI Qualified Name)** – Kann bis zu 255 Zeichen lang sein und hat das folgende Format:

  `iqn.<Jahr–Mo>.<umgekehrter_Domänenname>:<eindeutiger_Name>,`

  wobei `<Jahr-Mo>` für das Jahr und den Monat stehen, in dem Ihr Domänenname registriert wurde, `<umgekehrter_Domainname>` der offizielle Name Ihrer Domäne in umgekehrter Reihenfolge, und `<eindeutiger_Name>` ist ein beliebiger Name, den Sie verwenden möchten, z. B. der Name Ihres Servers.

  Beispiel: `iqn.1998-01.com.mycompany:myserver`.

- **EUI (Extended Unique Identifier, Erweiterter eindeutiger Bezeichner)** – Enthält das `eui.`-Präfix sowie einen Namen aus 16 Zeichen. Zum Namen gehören 24 Bits für den Firmennamen, die von der IEEE zugewiesen wurden, und 40 Bits für einen eindeutigen Bezeichner wie z. B. die Seriennummer.

Erkennung von Speicherressourcen

Um festzustellen, welche Speicher-Ressourcen im Netzwerk für den Zugriff verfügbar sind, verwenden die vom ESX Server-System unterstützten iSCSI-Initiatoren die folgenden Erkennungsmethoden:

- **Dynamische Erkennung** – Der Initiator erkennt iSCSI-Ziele durch Übermittlung einer *Targets versenden*-Anfrage an eine angegebene Zieladresse. Geben Sie dazu die Adresse des Zielgerätes ein, sodass der Initiator eine Erkennungssitzung mit diesem Ziel aufnehmen kann. Das Zielgerät antwortet durch die Weiterleitung einer Liste aller zusätzlichen Ziele, auf die der Initiator zugreifen kann.

- **Statische Erkennung** – Wenn das Zielgerät der Targets versenden-Session die Liste verfügbarer Ziele übermittelt hat, erscheinen diese im Verzeichnis „Statische Erkennung“. Diese Liste kann manuell um beliebige zusätzliche Ziele ergänzt oder um nicht benötigte Ziele reduziert werden.

  Die statische Erkennung steht nur für hardware-initiierten Speicher zur Verfügung.

iSCSI-Sicherheit

Da iSCSI die IP-Netzwerke zur Anbindung an entfernte Ziele verwendet, muss die Sicherheit der Verbindung gewährleistet werden. Das IP-Protokoll schützt die Daten, die es übermittelt, nicht selbst und kann auch die Legitimität der Initiatoren, die auf die Ziele im Netzwerk zugreifen, nicht überprüfen. Zur Sicherstellung der Sicherheit in IP-Netzwerken müssen Sie gesonderte Maßnahmen ergreifen.

ESX Server unterstützt das Challenge Handshake Authentication Protocol (CHAP), das die iSCSI-Initiatoren zur Authentifizierung nutzen können. Nach Aufnahme der ursprünglichen Verbindung mit dem Ziel durch den Initiator überprüft CHAP die Identität des Initiators und prüft den CHAP-Schlüssel, den sowohl der Initiator als auch das Ziel haben. Das kann während der iSCSI-Sitzung regelmäßig wiederholt werden.

Achten Sie bei der Konfiguration der iSCSI-Initiatoren für das ESX Server-System darauf, dass CHAP aktiviert ist. Weitere Informationen finden Sie unter „Absicherung von iSCSI-Speicher“ auf Seite 204.

Konfigurieren von mittels Hardware ausgelöster iSCSI-Speicherung

Mit dem Hardware-basierten iSCSI-Speicher werden spezielle Adapter von Drittanbietern verwendet, die über TCP/IP auf iSCSI-Speicher zugreifen können. Dieser iSCSI-Adapter kümmert sich um die gesamte iSCSI-Verarbeitung und -Verwaltung für das ESX Server-System.

Installieren und konfigurieren Sie den iSCSI-Hardware-Adapter vor der Einrichtung des Datastores auf dem iSCSI-Speichergerät.

Folgende Anleitungen helfen Ihnen bei der Vorbereitung und Einrichtung von Datastores, auf die Sie über die iSCSI-Hardware-Verbindung zugreifen:

- „Installation des iSCSI-Hardware-Initiators“ auf Seite 114
- „Anzeige der Eigenschaften des iSCSI-Hardware-Initiators“ auf Seite 114
- „Konfiguration eines iSCSI-Hardware-Initiators“ auf Seite 115
- „Hinzufügen von hardware-initiiertem iSCSI-Speicher“ auf Seite 120

Installation des iSCSI-Hardware-Initiators

Bei ESX Server 3.0 benötigt das Host-System für iSCSI-Übertragungen den HBA QLogic QLA4010 iSCSI.

Weitere Informationen finden Sie im *Handbuch der I/O-Kompatibilität* auf der VMware Website unter **www.vmware.com**.

Weitere Informationen zum Erwerb und zur Installation des Adapters finden Sie auf der QLogic-Website unter **www.qlogic.com**.

Anzeige der Eigenschaften des iSCSI-Hardware-Initiators

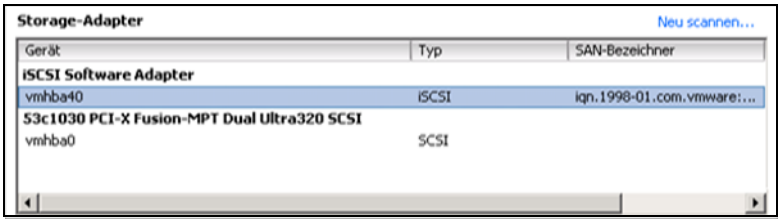
Bevor Sie mit der Konfiguration des iSCSI-Hardware-Initiators beginnen, überprüfen Sie, dass der iSCSI-HBA ordnungsgemäß installiert wurde und im Verzeichnis der Adapter, die konfiguriert werden können, aufgelistet wird. Wenn der Initiator installiert wurde, können Sie seine Eigenschaften anzeigen.

Anzeige der Eigenschaften des iSCSI-Hardware-Initiators

1 Melden Sie sich am VMware VI Client an und wählen Sie einen Server aus dem Inventar aus.

2 Klicken Sie auf die Registerkarte **Konfiguration** und klicken Sie unter Hardware auf **Speicheradapter**.

Ein Verzeichnis der verfügbaren Speicheradapter wird angezeigt. In diesem Verzeichnis befindet sich auch der iSCSI-HBA.

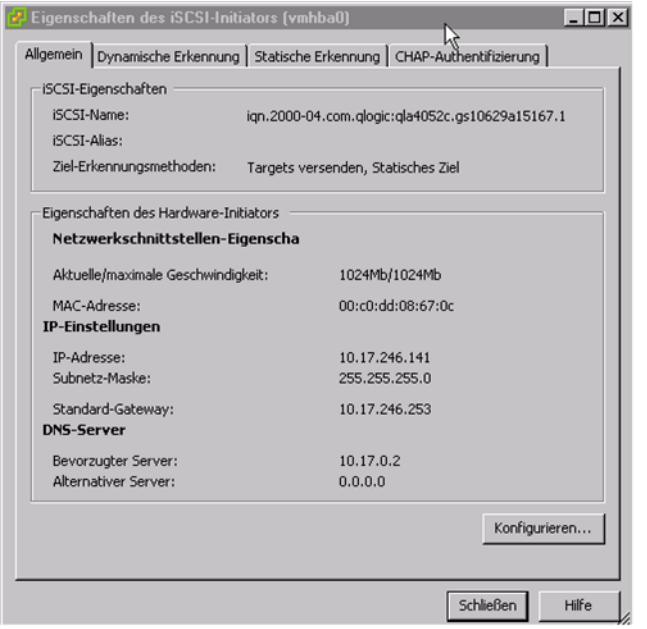


3 Wählen Sie unter „HBA“ den Initiator aus, den Sie konfigurieren möchten.

Es werden die Details zu diesem Initiator angezeigt, u. a. das Modell, die IP-Adresse, der iSCSI-Name, die Zielerkennung, das iSCSI-Alias und erkannte Ziele.

4 Klicken Sie auf **Eigenschaften**.

Das Dialogfeld **iSCSI-Initiator-Eigenschaften** wird geöffnet. Auf der Registerkarte **Allgemein** werden zusätzliche Merkmale des Initiators angezeigt.



Sie können den Hardware-Initiator jetzt konfigurieren oder seine Standardmerkmale ändern.

Konfiguration eines iSCSI-Hardware-Initiators

Während der Konfiguration des iSCSI-Hardware-Initiators müssen Sie den iSCSI-Namen, die IP-Adressen, die Zieladressen und die CHAP-Parameter des Initiators einrichten. Weitere Informationen finden Sie in folgenden Abschnitten:

- „Einrichten von Namensparametern für iSCSI-Hardware-Initiatoren“ auf Seite 115
- „Einrichten von Erkennungsadressen für Hardware-Initiatoren“ auf Seite 117
- „Einrichten von CHAP-Parametern für Hardware-Initiatoren“ auf Seite 118

Nach der Konfiguration des iSCSI-Hardware-Initiators müssen Sie erneut nach Speicher-Devices scannen, damit alle LUNs, auf die der Initiator zugreifen kann, im Verzeichnis der für Ihren ESX Server-Host verfügbaren Speicher-Devices aufgelistet wird. Weitere Informationen finden Sie unter „Neu scannen“ auf Seite 131.

Einrichten von Namensparametern für iSCSI-Hardware-Initiatoren

Stellen Sie beim Konfigurieren der iSCSI-Hardware-Initiatoren sicher, dass ihre Namen und IP-Adressen richtig formatiert sind.

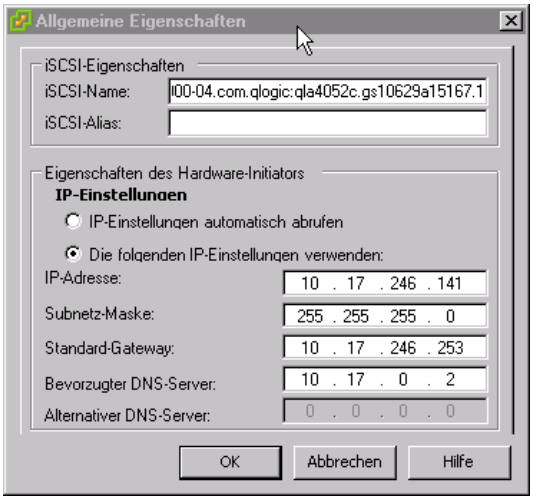
Weitere Informationen finden Sie unter „Namenskonventionen“ auf Seite 112.

So richten Sie den iSCSI-Namen und die IP-Adresse für den Hardware-Initiator ein.

1 Öffnen Sie das Dialogfeld **iSCSI-Initiator-Eigenschaften** entsprechend der Anleitung unter „Anzeige der Eigenschaften des iSCSI-Hardware-Initiators“ auf Seite 114.

2 Klicken Sie auf **Konfigurieren**.

Das Dialogfeld **Allgemeine Eigenschaften** wird geöffnet.



3 Wenn Sie den Standard-iSCSI-Namen für den Initiator ändern möchten, geben Sie einen neuen Namen ein.

Stellen Sie sicher, dass der Name den Namenskonventionen entspricht, sonst erkennen ggf. bestimmte Speichergeräte den iSCSI-Hardware-Initiator nicht.

4 Geben Sie das iSCSI-Alias ein.

Das Alias ist ein benutzerfreundlicher Name, der zur Identifizierung des iSCSI-Hardware-Initiators verwendet wird.

5 Wählen Sie unter **Eigenschaften des Hardware-Initiators** eine der folgenden Optionen aus:

- **IP-Einstellungen automatisch abrufen**
- **Die folgende IP-Einstellungen verwenden**

6 Wenn Sie **Die folgende IP-Einstellungen verwenden** ausgewählt haben, müssen Sie die folgenden Werte eingeben:

- **IP-Adresse**
- **Subnet-Maske**

- **Standard-Gateway**
- **Bevorzugter DNS-Server**
- **Alternativer DNS-Server** (optional)

7 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Einrichten von Erkennungsadressen für Hardware-Initiatoren

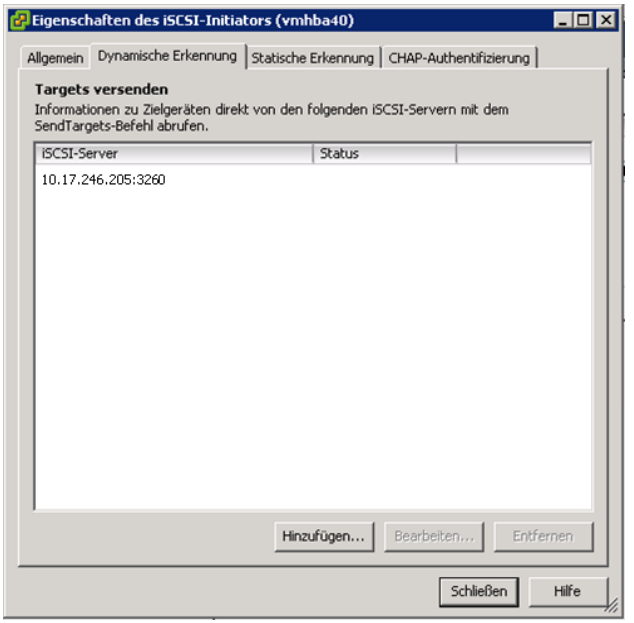
Sie müssen Zielerkennungsadressen einrichten, um den Hardware-Initiator in die Lage zu versetzen zu erkennen, welche Speicher-Ressource auf dem Netzwerk zur Verfügung stehen.

Weitere Informationen finden Sie unter „Erkennung von Speicherressourcen“ auf Seite 112.

Einrichtung von Zielerkennungsadressen für den Hardware-Initiator

1 Öffnen Sie das Dialogfeld **iSCSI-Initiator-Eigenschaften** entsprechend der Anleitung unter „Anzeige der Eigenschaften des iSCSI-Hardware-Initiators“ auf Seite 114.

2 Klicken Sie im Dialogfeld **iSCSI-Initiator-Eigenschaften** auf die Registerkarte **Dynamische Erkennung**.



3 Klicken Sie auf **Hinzufügen**, um ein neues iSCSI-Ziel, das der ESX Server-Host für eine Targets versenden-Session verwenden kann, hinzuzufügen.

Daraufhin wird das Dialogfeld **Server als Sendeziele hinzufügen** angezeigt.

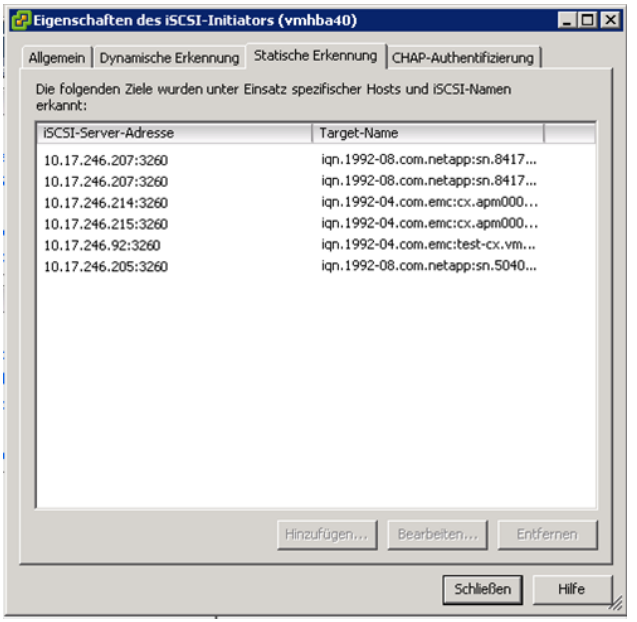
4 Geben Sie die Daten des Ziels ein und klicken Sie auf **OK**.

Nachdem der ESX Server-Host eine Targets versenden-Session mit dem Zielgerät aufgebaut hat, werden alle neu erkannten Ziele im Verzeichnis **Statische Erkennung** angezeigt.

5 Um ein bestimmtes Ziel zu ändern oder zu löschen, markieren Sie das Ziel und klicken Sie auf **Bearbeiten** oder **Entfernen**.

6 Klicken Sie auf die Registerkarte **Statische Erkennung**.

Die Registerkarte zeigt alle dynamisch erkannten Ziele an.



7 Um ein Ziel hinzuzufügen, auf das der ESX Server-Host zugreifen kann, klicken Sie auf **Hinzufügen** und geben Sie die Daten des Ziels ein.

8 Wenn Sie ein bestimmtes dynamisch erkanntes Ziel ändern oder löschen möchten, markieren Sie das Ziel und klicken Sie auf **Bearbeiten** oder **Entfernen**.

HINWEIS Wenn Sie ein dynamisch erkanntes statisches Ziel entfernen, kann das Ziel entweder beim nächsten Scan, beim Zurücksetzen des HBAs oder durch einen Neustart des Systems erneut zur Liste hinzugefügt werden.

Einrichten von CHAP-Parametern für Hardware-Initiatoren

Achten Sie bei der Konfiguration des iSCSI-Hardware-Initiators darauf, dass die CHAP-Parameter für den Initiator aktiviert sind. Sollten die Parameter nicht aktiviert sein, müssen Sie diese konfigurieren.

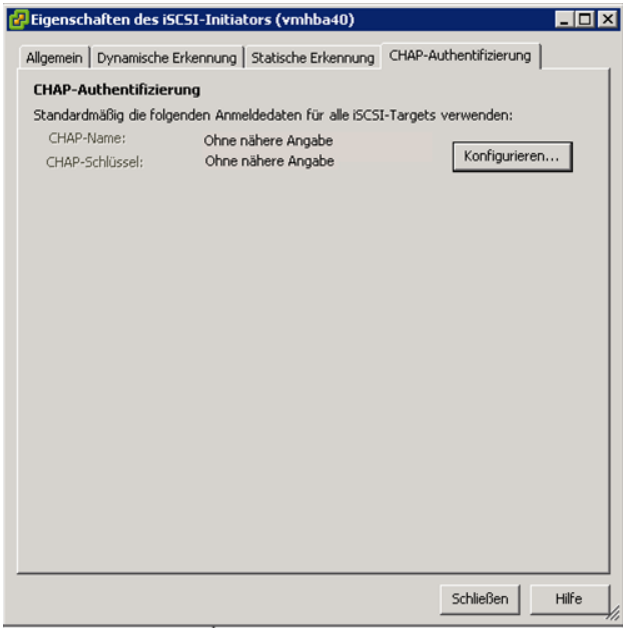
Weitere Informationen finden Sie unter „iSCSI-Sicherheit“ auf Seite 113.

Einrichtung der CHAP-Parameter für den Hardware-Initiator

1 Öffnen Sie das Dialogfeld **iSCSI-Initiator-Eigenschaften** entsprechend der Anleitung unter „Anzeige der Eigenschaften des iSCSI-Hardware-Initiators“ auf Seite 114.

2 Klicken Sie auf die Registerkarte **CHAP-Authentifizierung**.

Die Registerkarte zeigt die Standard-CHAP-Parameter an.



3 Klicken Sie auf **Konfigurieren**, wenn Sie die bestehenden CHAP-Parameter ändern möchten.

Das Dialogfeld **CHAP-Authentifizierung** wird geöffnet.

4 Damit CHAP auch weiterhin aktiviert bleibt, muss **Die folgenden CHAP-Anmeldedaten verwenden** aktiviert sein.

5 Um einen neuen CHAP-Namen zu verwenden, deaktivieren Sie das Kontrollkästchen **Initiatornamen verwenden** und geben Sie einen anderen Namen ein.

6 Geben Sie bei Bedarf einen CHAP-Schlüssel an.

Alle neuen Ziele werden diesen CHAP-Schlüssel verwenden, um den Initiator zu authentifizieren.

7 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

HINWEIS Wenn Sie CHAP deaktivieren, werden alle Sitzungen, die eine CHAP-Authentifizierung erfordern, sofort beendet.

Hinzufügen von hardware-initiiertem iSCSI-Speicher

Wenn Sie einen Datastore auf einem Hardware-initiierten SCSI-Speicher-Device erstellen, führt Sie der **Assistent zum Hinzufügen von Speicher** durch die Konfiguration

Erstellung eines Datastores auf einem hardware-initiierten iSCSI-Gerät

1 Melden Sie sich am VMware VI Client an und wählen Sie einen Server aus dem Inventar aus.

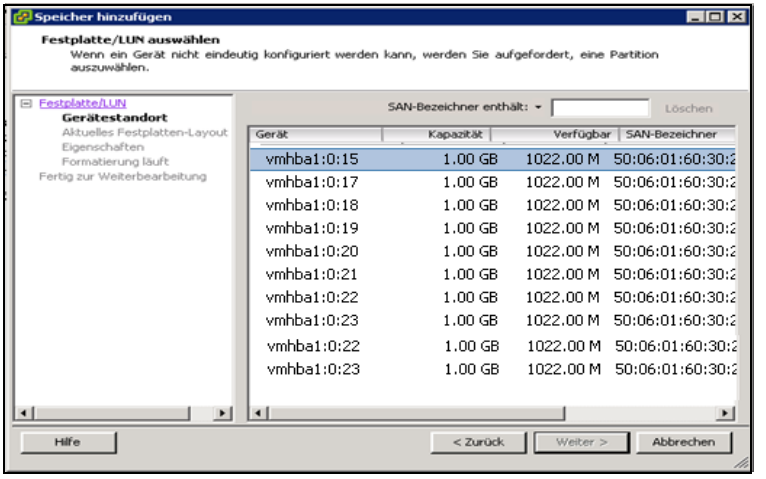
2 Klicken Sie auf die Registerkarte **Konfiguration** und klicken Sie unter Hardware auf **Speicher (SCSI, SAN und NFS)**.

3 Klicken Sie auf **Speicher hinzufügen**.

Das Dialogfeld **Speichertyp auswählen** wird angezeigt.

4 Markieren Sie den Speichertyp **Disk/LUN** (Festplatte/LUN) und klicken Sie auf **Weiter**.

Das Dialogfeld „**Disk/LUN** (Festplatte/LUN)“ wird angezeigt.



5 Wählen Sie das iSCSI-Gerät aus, das Sie für den Datastore verwenden möchten, und klicken Sie auf **Weiter**.

Das **Aktuelle Festplatten-Layout** wird angezeigt.

6 Überprüfen Sie das aktuelle Festplatten-Layout und klicken Sie auf **Weiter**.

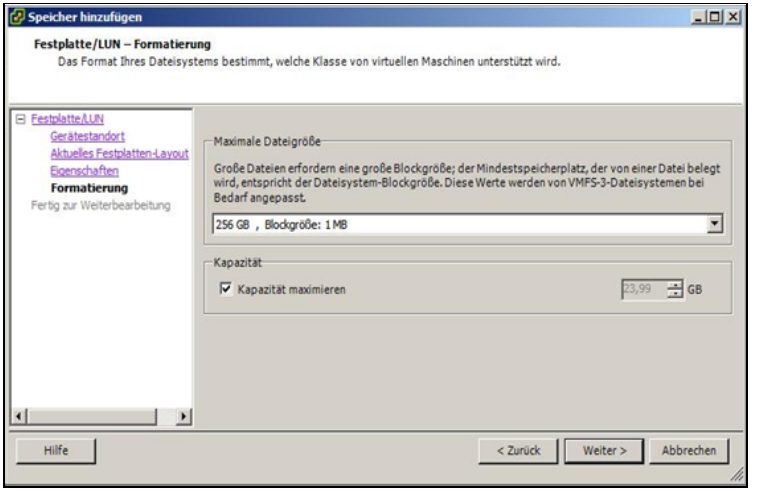
Das Dialogfeld **Festplatte/LUN–Eigenschaften** wird angezeigt.

7 Geben Sie einen Namen für den Datastore ein.

Der Name des Datastores wird im VI Client angezeigt. Die Bezeichnung muss in der vorliegenden Instanz der virtuellen Infrastruktur eindeutig sein.

8 Klicken Sie auf **Weiter**.

Das Dialogfeld **Festplatte/LUN–Formatierung** wird angezeigt.



9 Ändern Sie bei Bedarf die Werte für das Dateisystem und die Größe des Datastores. Standardmäßig wird der gesamte freie Speicherplatz des Speichergerätes angeboten.

10 Klicken Sie auf **Weiter**.

Das Dialogfeld **Übersicht** wird angezeigt.

11 Überprüfen Sie die Daten für den Datastore und klicken Sie auf **Fertig stellen**.

Dadurch wird ein Datastore auf einem hardware-initiierten iSCSI-Gerät erstellt.

12 Scannen Sie nach neuen Speichergeräten.

Weitere Informationen finden Sie unter „Neu scannen“ auf Seite 131.

Konfiguration von software-initiiertem iSCSI-Speicher

Bei der Verwendung von software-basiertem iSCSI können Sie einen normalen Netzwerkadapter verwenden, um das ESX Server-System an ein entferntes iSCSI-Ziel im IP-Netzwerk anzubinden. Der in das VMkernel integrierte Software-iSCSI-Initiator von ESX Server ermöglicht diese Verbindung, indem er über den Protokollstapel mit dem Netzwerkadapter kommuniziert.

Vor der Konfiguration des software-basierten iSCSI-Speichers muss die Netzwerkverbindung aktiviert und der iSCSI-Software-Initiator konfiguriert werden.

Gehen Sie bei der Vorbereitung und Einrichtung der Datastores, die eine Software-initiierte iSCSI-Verbindung zum Zugriff auf den iSCSI-Speicher verwenden, wie folgt vor:

1 Konfigurieren Sie den TCP/IP-Protokollstapel des Vmkernels.

Weitere Informationen finden Sie unter „Konfiguration des VMkernels“ auf Seite 33 und „Netzwerkkonfiguration für den Software iSCSI Speicher“ auf Seite 70.

2 Öffnen Sie einen Firewall-Port, indem Sie den iSCSI-Software-Client-Dienst aktivieren.

Siehe „Freigeben von Firewall-Ports für unterstützte Dienste und Management-Agenten“ auf Seite 192.

3 Konfigurieren Sie den iSCSI-Software-Initiator.

Siehe „Konfiguration eines iSCSI-Software-Initiators“ auf Seite 124.

4 Scannen Sie nach neuen iSCSI-LUNs.

Weitere Informationen finden Sie unter „Neu scannen“ auf Seite 131.

5 Richten Sie den Datastore ein.

Siehe „Hinzufügen von software-initiiertem iSCSI-Speicher“ auf Seite 129.

Anzeige der Eigenschaften des iSCSI-Software-Initiators

Der Software-iSCSI-Adapter, den das ESX Server-System verwendet, um auf software-initiierte iSCSI-Speichergeräte zuzugreifen, wird in der Liste der verfügbaren Adapter angezeigt. Sie können seine Eigenschaften mit dem VI Client anzeigen.

Anzeige der Eigenschaften des iSCSI-Software-Initiators

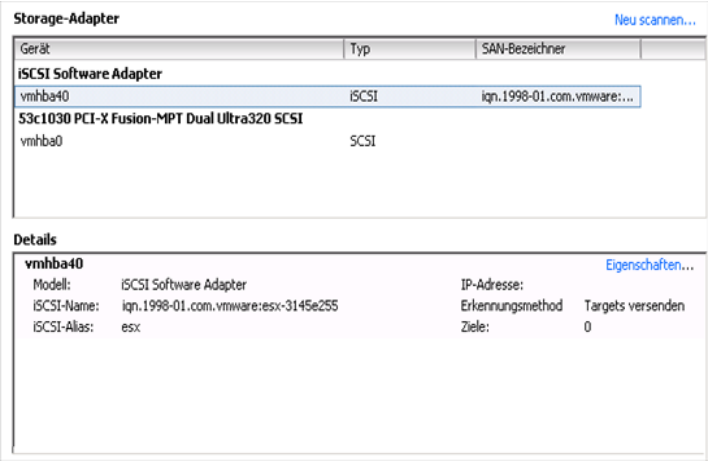
1 Melden Sie sich am VMware VI Client an und wählen Sie einen Server aus dem Inventar aus.

2 Klicken Sie auf die Registerkarte **Konfiguration** und klicken Sie unter Hardware auf **Speicheradapter**.

Ein Verzeichnis der verfügbaren Speicheradapter wird angezeigt.

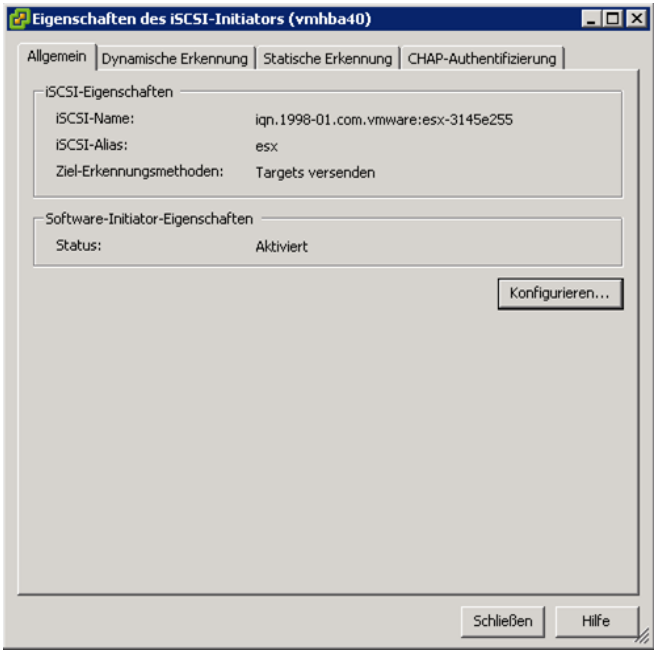
3 Wählen Sie den entsprechenden Software-Initiator unter „**iSCSI Software-Adapter** (iSCSI-Software-Adapter)“ aus.

Es werden die Details zu diesem Initiator angezeigt, u. a. das Modell, die IP-Adresse, der iSCSI-Name, die Zielerkennung, das iSCSI-Alias und erkannte Ziele.



4 Klicken Sie auf **Eigenschaften**.

Das Dialogfeld **iSCSI-Initiator-Eigenschaften** wird geöffnet. Auf der Registerkarte **Allgemein** werden zusätzliche Merkmale des Software-Initiators angezeigt.



Sie können den Software-Initiator jetzt konfigurieren oder seine Standardmerkmale ändern.

Konfiguration eines iSCSI-Software-Initiators

Während der Konfiguration des iSCSI-Software-Initiators müssen Sie den Initiator aktivieren und die Zieladressen und CHAP-Parameter des Initiators einrichten. Weitere Informationen finden Sie in folgenden Abschnitten:

- „Aktivieren von iSCSI-Software-Initiatoren“ auf Seite 125
- „Einrichten von Erkennungsadressen für Software-Initiatoren“ auf Seite 126
- „Einrichten von CHAP-Parametern für Software-Initiatoren“ auf Seite 127

Nach der Konfiguration des iSCSI-Software-Initiators müssen Sie erneut nach Speicher-Devices scannen, damit alle LUNs, auf die der Initiator zugreifen kann, im Verzeichnis der für ESX Server verfügbaren Speicher-Devices aufgelistet wird. Weitere Informationen finden Sie unter „Neu scannen“ auf Seite 131.

Aktivieren von iSCSI-Software-Initiatoren

Damit ESX Server den iSCSI-Software-Initiator verwenden kann, müssen Sie diesen zuerst aktivieren.

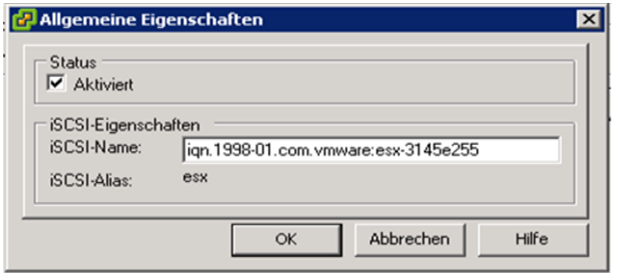
Aktivierung des iSCSI-Software-Initiators

1 Öffnen Sie das Dialogfeld **iSCSI-Initiator-Eigenschaften** entsprechend der Anleitung unter „Anzeige der Eigenschaften des iSCSI-Software-Initiators“ auf Seite 122.

2 Klicken Sie auf **Konfigurieren**.

Das Dialogfeld **Allgemeine Eigenschaften** wird geöffnet. Hier finden Sie den Status des Initiators, den Standardnamen und das Alias.

3 Aktivieren Sie das Kontrollkästchen **Aktiviert**, um den Initiator zu aktivieren.



4 Wenn Sie den Standard-iSCSI-Namen für den Initiator ändern möchten, geben Sie einen neuen Namen ein.

Stellen Sie sicher, dass der Name den Namenskonventionen entspricht, sonst erkennen ggf. bestimmte Speichergeräte den iSCSI-Software-Initiator nicht. Weitere Informationen finden Sie unter „Namenskonventionen“ auf Seite 112.

5 Geben Sie ein iSCSI-Alias ein oder ändern Sie das bestehende Alias.

Das Alias ist ein benutzerfreundlicher Name, der zur Identifizierung des iSCSI-Hardware-Initiators verwendet wird.

6 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Einrichten von Erkennungsadressen für Software-Initiatoren

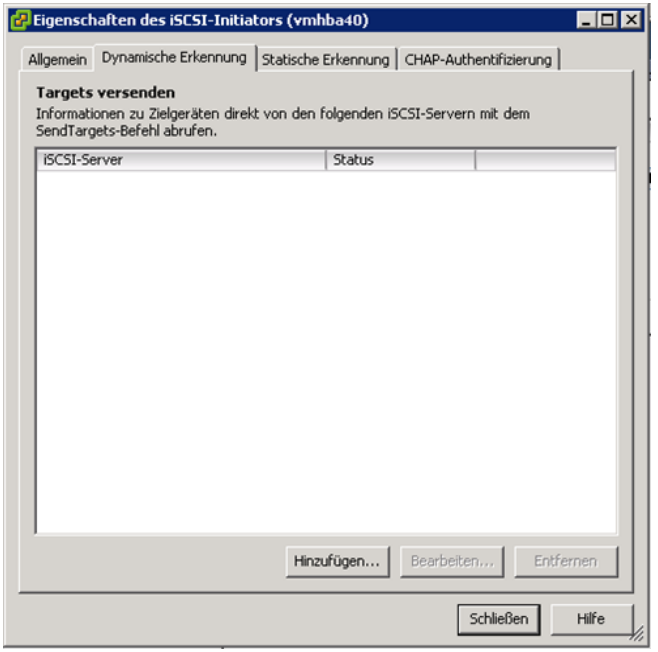
Sie müssen Zielerkennungsadressen einrichten, damit der Software-Initiator erkennen kann, welche Speicher-Ressource auf dem Netzwerk zur Verfügung steht.

Weitere Informationen finden Sie unter „Erkennung von Speicherressourcen“ auf Seite 112.

So richten Sie Zielerkennungsadressen für den Software-Initiator ein:

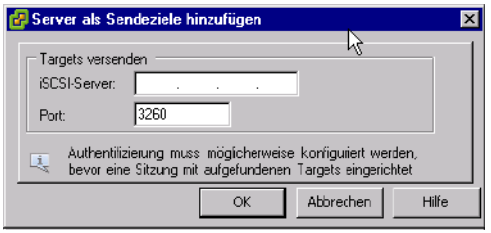
1 Öffnen Sie das Dialogfeld **iSCSI-Initiator-Eigenschaften** entsprechend der Anleitung unter „Anzeige der Eigenschaften des iSCSI-Software-Initiators“ auf Seite 122.

2 Klicken Sie auf die Registerkarte **Dynamische Erkennung**.



3 Klicken Sie auf **Hinzufügen**, um ein neues iSCSI-Ziel, das der ESX Server-Host für eine Targets versenden-Session verwenden kann, hinzuzufügen.

Das Dialogfeld **Ziel-senden-Server hinzufügen** wird angezeigt.



4 Geben Sie die Server-IP-Adresse für „Targets versenden“ ein und klicken Sie auf **OK**.

5 Wenn Sie einen bestimmten Ziel-senden-Server ändern oder löschen möchten, markieren Sie den Server und klicken Sie auf **Bearbeiten** oder **Entfernen**.

Einrichten von CHAP-Parametern für Software-Initiatoren

Achten Sie bei der Konfiguration des iSCSI-Software-Initiators darauf, dass die CHAP-Parameter für den Initiator aktiviert sind. Sollten die Parameter nicht aktiviert sein, müssen Sie diese konfigurieren.

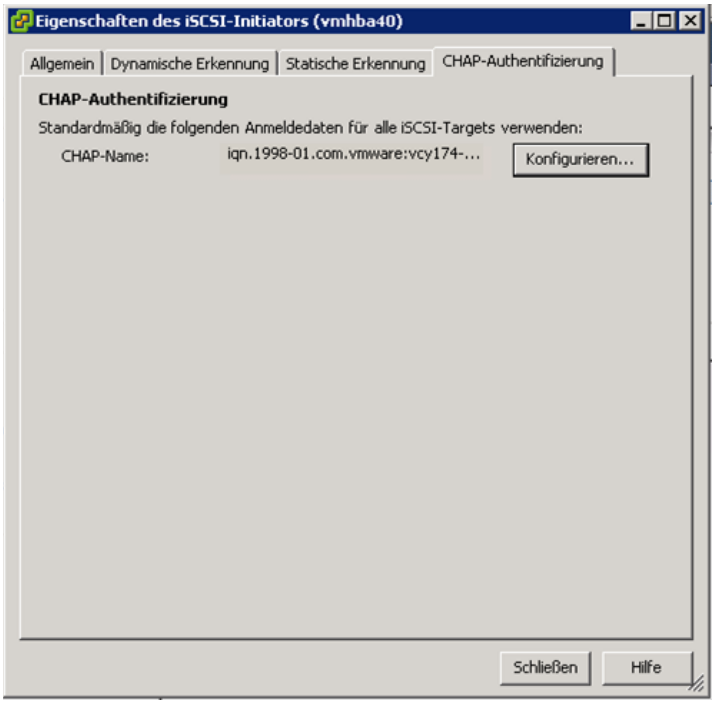
Weitere Informationen finden Sie unter „iSCSI-Sicherheit“ auf Seite 113.

Einrichtung der CHAP-Parameter für den Software-Initiator

1 Öffnen Sie das Dialogfeld „iSCSI-Initiator-Eigenschaften“ entsprechend der Anleitung unter „Anzeige der Eigenschaften des iSCSI-Software-Initiators“ auf Seite 122.

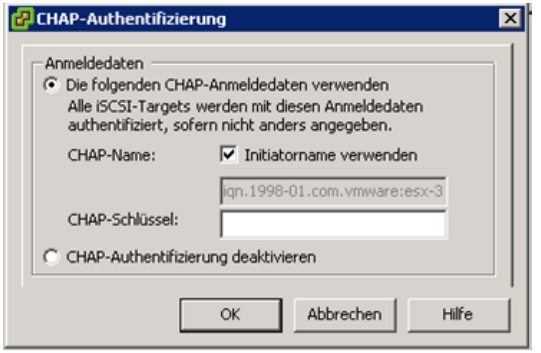
2 Klicken Sie auf die Registerkarte **CHAP Authentifizierung**.

Die Registerkarte zeigt die Standard-CHAP-Parameter an.



3 Klicken Sie auf **Konfigurieren**, wenn Sie die bestehenden CHAP-Parameter ändern möchten.

Das Dialogfeld **CHAP-Authentifizierung** wird geöffnet.



4 Damit CHAP auch weiterhin aktiviert bleibt, muss **Die folgenden CHAP-Anmeldedaten verwenden** aktiviert sein.

5 Um einen neuen CHAP-Namen zu verwenden, deaktivieren Sie das Kontrollkästchen **Initiatornamen verwenden** und geben Sie einen anderen Namen ein.

6 Geben Sie bei Bedarf einen CHAP-Schlüssel an.

Alle neuen Ziele werden diesen CHAP-Schlüssel verwenden, um den Initiator zu authentifizieren. Bereits bestehende Sitzungen sind davon nicht betroffen.

7 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

HINWEIS Wenn Sie CHAP deaktivieren, werden alle Sitzungen, die eine CHAP-Authentifizierung erfordern, sofort beendet.

Hinzufügen von software-initiiertem iSCSI-Speicher

Wenn Sie einen Datastore auf einem Software-initiierten SCSI-Speicher-Device erstellen, führt Sie der **Assistent zum Hinzufügen von Speicher** durch die Konfiguration.

Erstellung eines Datastores auf einem software-initiierten iSCSI-Gerät

1 Melden Sie sich am VMware VI Client an und wählen Sie einen Server aus dem Inventar aus.

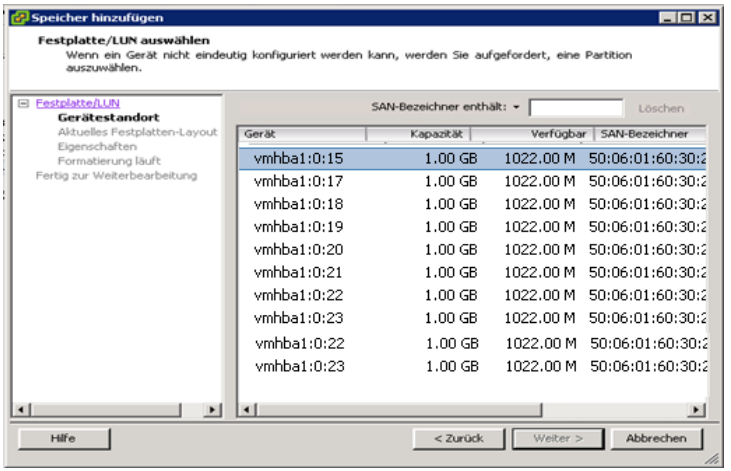
2 Klicken Sie auf die Registerkarte **Konfiguration** und klicken Sie unter Hardware auf **Speicher (SCSI, SAN und NFS)**.

3 Klicken Sie auf **Speicher hinzufügen**.

Das Dialogfeld **Speichertyp auswählen** wird angezeigt.

4 Markieren Sie den Speichertyp **Disk/LUN** (Festplatte/LUN) und klicken Sie auf **Weiter**.

Das Dialogfeld **Disk/LUN** (Festplatte/LUN) wird angezeigt.



5 Wählen Sie das iSCSI-Gerät aus, das Sie für den Datastore verwenden möchten, und klicken Sie auf **Weiter**.

Das **Aktuelle Festplatten-Layout** wird angezeigt.

6 Überprüfen Sie das aktuelle Festplatten-Layout und klicken Sie auf **Weiter**.

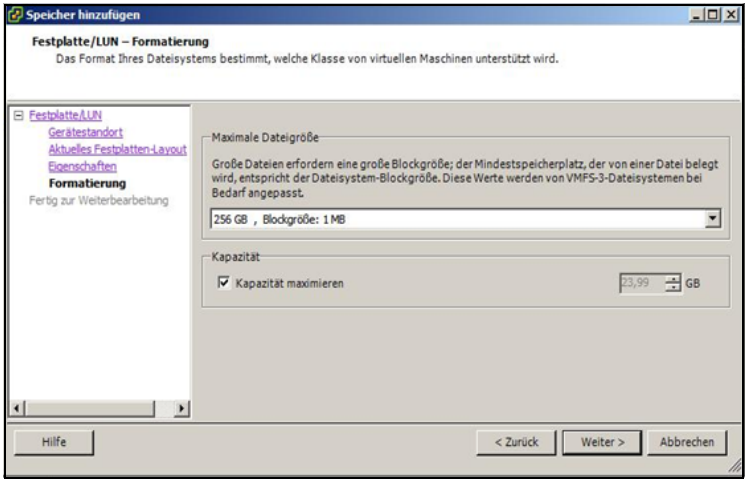
Das Dialogfeld **Festplatte/LUN–Eigenschaften** wird angezeigt.

7 Geben Sie einen Namen für den Datastore ein.

Der Name des Datastores wird im VI Client angezeigt. Die Bezeichnung muss in der vorliegenden Instanz der virtuellen Infrastruktur eindeutig sein.

8 Klicken Sie auf **Weiter**.

Das Dialogfeld **Festplatte/LUN–Formatierung** wird angezeigt.



9 Ändern Sie bei Bedarf die Werte für das Dateisystem und die Größe des Datastores.

Standardmäßig wird der gesamte freie Speicherplatz des Speichergerätes angeboten.

10 Klicken Sie auf **Weiter**.

Das Dialogfeld **Fertig stellen** wird angezeigt.

11 Überprüfen Sie die Konfigurationsdaten für den Datastore und klicken Sie auf **Fertig stellen**.

Dadurch wird ein Datastore auf einem software-initiierten iSCSI-Speichergerät erstellt.

12 Scannen Sie nach neuen Speichergeräten.

Weitere Informationen finden Sie unter „Neu scannen“ auf Seite 131.

Neu scannen

Wenn eine neue LUN über einen Adapter neu zur Verfügung steht, registriert ESX Server dieses neue virtuelle Gerät zur Verwendung durch die virtuellen Maschinen. Wenn eine bestehende LUN nicht länger verwendet wird und nicht mehr da zu sein scheint, wird es von der Liste der für die virtuellen Maschinen zur Verfügung stehenden Geräte entfernt.

Ein erneuter Scan wird in folgenden Fällen empfohlen:

- Wenn Änderungen an den Speicherfestplatten oder LUNs, die dem ESX Server-System zur Verfügung stehen, vorgenommen wurde

- Wenn Änderungen an den Speicheradaptern vorgenommen wurden
- Wenn neue Datastores erstellt werden
- Wenn bestehende Datastores bearbeitet oder entfernt werden

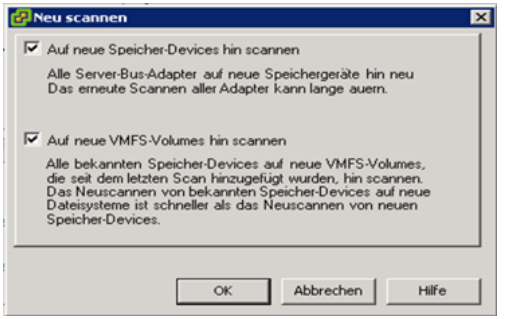
Neu scannen

1 Markieren Sie im VI Client einen Host und klicken Sie auf die Registerkarte **Konfiguration**.

2 Wählen Sie unter „Hardware“ die Option **Speicheradapter** und klicken Sie oberhalb des Bereichs **Speicheradapter** auf **Neu scannen**.

HINWEIS Sie können auch einen einzelnen Adapter markieren und auf **Neu scannen** klicken, wenn Sie nur diesen Adapter scannen möchten.

Das Dialogfeld **Neu scannen** wird geöffnet.


Neu scannen
Auf neue Speicher-Devices hin scannen
Alle Server-Bus-Adapter auf neue Speichergeräte hin neu
Das erneute Scannen aller Adapter kann lange auern.
Auf neue VMFS-Volumes hin scannen
Alle bekannten Speicher-Devices auf neue VMFS-Volumes,
die seit dem letzten Scan hinzugefügt wurden, hin scannen.
Das Neuscannen von bekannten Speicher-Devices auf neue
Dateisysteme ist schneller als das Neuscannen von neuen
Speicher-Devices.
OK
Abbrechen
Hilfe

3 Wenn neue Festplatten oder LUNs erkannt werden sollen, aktivieren Sie **Auf neue Speicher-Devices hin scannen**.

Wenn neue LUNs erkannt werden, werden Sie im Verzeichnis der Festplatten und LUNs angezeigt.

4 Wenn neue Datastores erkannt werden sollen, aktivieren Sie **Auf neue VMFS-Datenträger scannen**.

Wenn neue Datastores oder VMFS-Datenträger erkannt werden, werden sie in der Liste der Datastores angezeigt.

NAS-Netzwerkspeicher

Dieser Abschnitt enthält folgende Informationen zu Network Attached Storage (NAS):

- „Gemeinsames Plattenspeichersystem“ auf Seite 133
- „Verwendung von NFS durch virtuelle Maschinen“ auf Seite 133
- „NFS-Volumes und Delegate-Benutzer virtueller Maschinen“ auf Seite 134

- „Konfiguration von ESX Server zum Zugriff auf NFS-Datenträger“ auf Seite 135
- „Erstellung eines NFS-basierten Datastores“ auf Seite 135

ESX Server unterstützt die Verwendung von Network Attached Storage (NAS) über das NFS-Protokoll. Für bestimmte Anwender ist NFS eventuell eine kostengünstigere Alternative zu einem SAN-Speicher.

Gemeinsames Plattenspeichersystem

ESX Server unterstützt die folgenden Funktionen eines gemeinsamen Plattenspeichersystems auf NAS-Volumes:

- Verwendung von VMotion. Verschieben von aktiven virtuellen Maschinen von einem ESX Server auf einen anderen ohne Unterbrechung des Betriebs.
- Erstellung von virtuellen Maschinen auf NFS-Datenträgern.
- Booten virtueller Maschinen, die auf NFS-Datenträgern gespeichert sind.
- Erstellung von Momentaufnahmen virtueller Maschinen auf NFS-Datenträgern. Erstellen Sie eine Momentaufnahme, wenn Sie den Status der virtuellen Maschine beibehalten möchten, um beliebig oft zu einem gleichen Status zurückkehren zu können.

Verwendung von NFS durch virtuelle Maschinen

Das von ESX Server unterstützte NFS-Protokoll ermöglicht die Kommunikation zwischen einem NFS-Client und einem NFS-Server. Der Client fordert Informationsanfragen von dem Server ab, der das Ergebnis ausgibt.

Über den in den ESX Server implementierten NFS-Client können Sie auf den NFS-Server zugreifen und NFS-Volumes verwenden, um virtuelle Maschinenfestplatten zu speichern. ESX Server unterstützt über TCP/IP nur NFS Version 3.

Mit dem VI Client können Sie NFS-Datenträger als Datastores konfigurieren. Konfigurierte NFS-Datastores werden im VI Client angezeigt und können genau wie VMFS-basierte Datastores zur Speicherung virtueller Festplattendateien verwendet werden.

Die von Ihnen auf NFS-basierten Datastores erstellten virtuellen Festplatten verwenden ein Festplattenformat, das vom NFS-Server vorgegeben wird. In der Regel ist dies ein Thin-Festplattenformat, das eine bedarfsgerechte Speicherplatzzuordnung erfordert. Wenn der Speicherplatz auf der virtuellen Maschine während des Schreibvorgangs auf die Festplatte nicht mehr ausreicht, erhalten Sie vom Virtual Infrastructure Client eine Benachrichtigung darüber, dass zusätzlicher Speicherplatz erforderlich ist. Sie können dann aus den folgenden Optionen wählen:

- Zusätzlichen Speicherplatz auf dem Volume freimachen, damit der Schreibvorgang auf die Festplatte fortgesetzt werden kann.

- Beenden der virtuellen Maschinensitzung. Durch das Beenden der Session wird die virtuelle Maschine heruntergefahren.

Die Abbildung Abbildung 6-4 zeigt eine virtuelle Maschine, die ein NFS-Volume zur Speicherung ihrer Dateien verwendet.

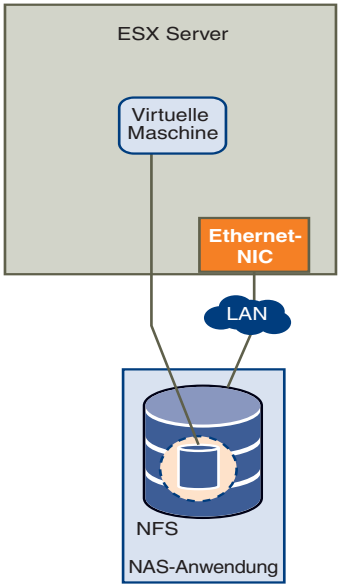


Abbildung 6-4. NFS-Speicher

In dieser Konfiguration stellt ESX Server eine Verbindung zum NFS-Server her, auf dem die virtuellen Festplattendateien gespeichert sind.

WARNHINWEIS Wenn ESX Server auf eine virtuelle Festplattendatei auf einem NFS-basierten Datastore zugreift, wird im gleichen Verzeichnis, in dem sich die Festplattendatei befindet, eine spezielle `ICK-XXX`-Sperrdatei erstellt, um zu verhindern, dass andere ESX Server-Hosts auf diese virtuelle Festplattendatei zugreifen. Diese `.lck-XXX`-Sperrdatei sollte nicht gelöscht werden, da sonst die aktive virtuelle Maschine nicht auf ihre Festplattendatei zugreifen kann.

NFS-Volumes und Delegate-Benutzer virtueller Maschinen

Wenn Sie virtuelle Maschinen auf einem NFS-basierten Datastore erstellen, konfigurieren oder verwalten möchten, müssen Sie einem bestimmten Benutzer, dem Delegate-Benutzer, NFS-Zugriffsrechte zuweisen.

Der Delegate-Benutzer für den ESX Server-Host ist standardmäßig `root`. Nicht alle NFS-Datastores akzeptieren jedoch `Root` als Delegate-Benutzer. In einigen Fällen ist es möglicherweise angebracht, dass der NFS-Administrator die Volumes mit aktivierter `root squash` Option exportiert, um die NFS-Volumes vor unbefugtem Zugriff zu schützen. Wenn die Option `root squash` aktiviert ist, behandelt der NFS-Server den Root-Zugriff wie einen unberechtigten Benutzerzugriff und verweigert möglicherweise den Zugriff des ESX Server-Hosts auf Dateien der virtuellen Maschine, die auf dem NFS-Volume gespeichert sind.

Sie können dem Delegate-Benutzer mithilfe der experimentellen ESX Server-Funktionen eine andere Identität zuweisen. Diese Identität muss mit der Identität des Inhabers des Verzeichnisses auf dem NFS-Server übereinstimmen. Ansonsten kann der ESX Server-Host keine Vorgänge auf Dateiebene durchführen.

Weitere Informationen zum Einrichten einer neuen Identität für den Delegate-Benutzer finden Sie unter „Delegierte der virtuellen Maschine für NFS-Speicher“ auf Seite 234.

WARNHINWEIS Das Ändern des Delegierten Anwenders für einen ESX Server-Host ist experimentell. Darüber hinaus bietet VMware derzeit nur eingeschränkten Support für diese Funktion. Die Verwendung dieser Funktion kann zu einem unerwarteten und unerwünschten Verhalten führen.

Konfiguration von ESX Server zum Zugriff auf NFS-Datenträger

Damit NFS auf Daten auf entfernten Servern zugreifen kann, muss es an das Netzwerk angebunden sein. Vor der Konfiguration von NFS muss daher zuerst die Netzwerkverbindung für VMotion und für den IP-Speicher konfiguriert werden.

Weitere Informationen zur Netzwerkkonfiguration finden Sie unter „Konfiguration des VMkernels“ auf Seite 33.

Erstellung eines NFS-basierten Datastores

Wenn Sie einen Datastore auf einem NFS-Datenträger erstellen, führt Sie der **Assistent zum Hinzufügen von Speicher** durch die Konfiguration.

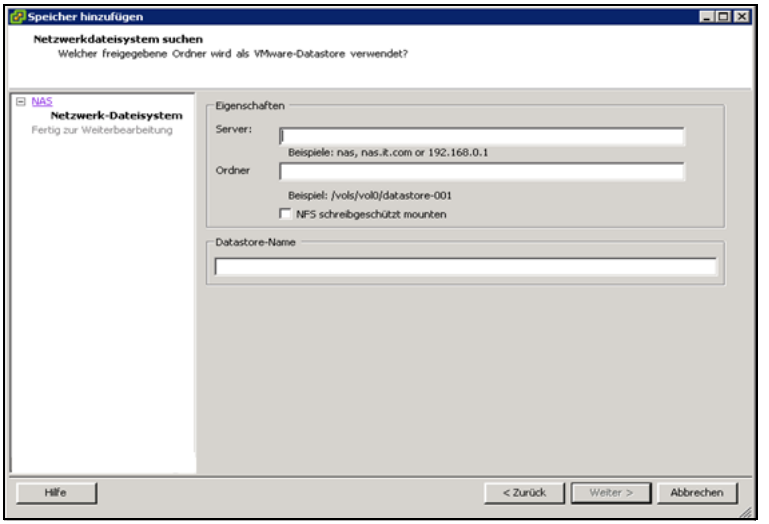
Einbindung eines NFS-Datenträgers

1. Melden Sie sich am VMware VI Client an und wählen Sie einen Server aus dem Inventar aus.
2. Klicken Sie auf die Registerkarte **Konfiguration** und klicken Sie unter Hardware auf **Speicher (SCSI, SAN und NFS)**.
3. Klicken Sie auf **Speicher hinzufügen**.

   Das Dialogfeld **Speichertyp auswählen** wird angezeigt.

4 Wählen Sie **Network File System (NFS)** als Speichertyp und klicken Sie auf **Weiter**.

Das Dialogfeld **NFS suchen** wird angezeigt.



5 Geben Sie den Server-Namen, den Mount-Punkt-Ordner und den Datastore-Namen ein.

6 Klicken Sie auf **Weiter**.

Das Dialogfeld **NFS-Übersicht** wird angezeigt.

7 Überprüfen Sie die Konfigurationsdaten und klicken Sie auf **Fertig stellen**.

7 Speicherverwaltung

Dieses Kapitel enthält Informationen zur Verwaltung bestehender Datastores und Dateisysteme, die Datastores bilden. Dieses Kapitel enthält folgende Abschnitte:

- „Verwaltung von Datastores und Dateisystemen“ auf Seite 138
- „Bearbeiten bestehender VMFS-basierter Datastores“ auf Seite 139
- „Verwalten von Pfaden für Fibre-Channel und iSCSI“ auf Seite 143
- „Die vmkfstools-Befehle“ auf Seite 150

Verwaltung von Datastores und Dateisystemen

Das ESX Server-System verwendet Datastores, um alle Dateien, die seinen virtuellen Maschinen zugeordnet sind, zu speichern. Der Datastore ist eine logische Speichereinheit, die Festplattenspeicher auf einem physischen Gerät, auf einer Festplattenpartition oder übergreifend auf mehreren physischen Geräten verwendet. Der Datastore kann sich auf verschiedenen Typen von physischen Geräten wie z. B. SCSI, iSCSI, Fibre-Channel-SANs oder NFS befinden.

HINWEIS Als Alternative zur Verwendung des Datastores kann Ihre virtuelle Maschine, über einer Zuordnungsdatei (RDM) als Proxy, direkt auf Raw-Devices zugreifen. Weitere Informationen über RDM-Zuordnungen finden Sie unter „Raw-Device-Mapping“ auf Seite 151.

Weitere Informationen zu Datastores finden Sie unter „Datastores und Dateisysteme“ auf Seite 90.

Es gibt zwei Möglichkeiten, dem VI Client Datastores hinzufügen:

- Erkennung beim Hinzufügen eines Hosts zum Inventar – Wenn Sie einen Host zum Inventar hinzufügen, zeigt der VI Client alle Datastores an, die der Host erkennt.
- Erstellung auf einem verfügbaren Speichergerät – Sie können mit dem Befehl **Speicher hinzufügen** einen neuen Datastore erstellen und konfigurieren.

Nach der Erstellung von Datastores können Sie diese dazu verwenden, VM-Dateien zu speichern. Gegebenenfalls können Sie die Datastores auch ändern. So können Sie zum Beispiel Erweiterungen für den Datastore hinzufügen oder Datastores umbenennen oder löschen.

Weitere Informationen finden Sie in folgenden Abschnitten:

- „Hinzufügen neuer Datastores“ auf Seite 138
- „Entfernen bestehender Datastores“ auf Seite 139

Hinzufügen neuer Datastores

Sie können einen Datastore auf einer Fibre-Channel-, iSCSI- oder einer lokalen SCSI-Festplatte erstellen. Sie kön nen auch einen NFS-Datenträger über eine Netzwerkverbindung einbinden und ihn als VMware Datastore verwenden. Wählen Sie zur Erstellung eines Datastores die Art des Datastores, den Sie erstellen möchten. Sie haben folgende Möglichkeiten:

- „Hinzufügen von lokalem SCSI-Speicher“ auf Seite 104
- „Hinzufügen von Fibre-Channel-Speicher“ auf Seite 108
- „Hinzufügen von hardware-initiiertem iSCSI-Speicher“ auf Seite 120
- „Hinzufügen von software-initiiertem iSCSI-Speicher“ auf Seite 129
- „Erstellung eines NFS-basierten Datastores“ auf Seite 135

Entfernen bestehender Datastores

Sie können Datastores, die Sie nicht mehr verwenden, entfernen.

VORSICHT Die Entfernung eines Datastores vom ESX Server-System unterbricht die Verbindung zwischen dem System und dem Speichergerät mit dem Datastore und hält alle Funktionen dieses Speichergerätes an.

Sie können Datastores nicht entfernen, wenn sie virtuelle Festplatten einer aktiven virtuellen Maschine enthalten.

Entfernen eines Datastores

1. Melden Sie sich am VMware VI Client an und wählen Sie einen Server aus dem Inventar aus.
2. Klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Speicher (SCSI, SAN und NFS)**.
3. Markieren Sie den Datastore, den Sie entfernen möchten, und klicken Sie auf **Entfernen**.
4. Bestätigen Sie, dass Sie den Datastore entfernen möchten.

Bearbeiten bestehender VMFS-basierter Datastores

Datastores im VMFS-Format werden auf SCSI-basierten Speichergeräten bereitgestellt.

Nach der Erstellung eines VMFS-basierten Datastores können Sie ihn ändern. Weitere Informationen finden Sie in folgenden Abschnitten:

- „Aktualisierung von Datastores“ auf Seite 139
- „Namensänderung von Datastores“ auf Seite 140
- „Erweiterung von Datastores“ auf Seite 141

Aktualisierung von Datastores

ESX Server 3 verfügt über eine neues Dateisystem, VMFS Version 3 (VMFS-3). Wenn Ihr Datastore in VMFS-2 formatiert wurde, können Sie die auf VMFS-2 gespeicherten Dateien zwar lesen, aber nicht verwenden. Dazu müssen Sie die Dateien von VMFS-2 auf VMFS-3 aktualisieren.

Bei der Aktualisierung von VMFS-2 auf VMFS-3 stellt der Datei-Sperrmechanismus von ESX Server sicher, dass während der Konvertierung kein Remote-ESX Server oder lokale Prozesse auf den VMFS-Datenträger zugreifen. ESX Server erhält alle Dateien auf dem Datastore.

Vor der Aktualisierung werden als Vorsichtsmaßnahme folgende Schritte empfohlen:

- Akzeptieren oder verwerfen Sie alle Änderungen an virtuellen Festplatten auf dem VMFS 2-Volume, für das ein Upgrade durchgeführt werden soll.

- Fertigen Sie ein Backup des VMFS-2-Datenträgers, den Sie aktualisieren möchten, an.
- Stellen Sie sicher, dass keine angeschalteten virtuellen Maschinen diesen VMFS-2-Datenträger verwenden.
- Stellen Sie sicher, dass kein anderer ESX Server auf diesen VMFS-2-Datenträger zugreift.
- Stellen Sie sicher, dass der VMFS-2-Datenträger nicht auf einem anderen ESX Server eingebunden ist.

VORSICHT
- Die Konvertierung von VMFS-2 in VMFS-3 ist nicht umkehrbar. Nach der Konvertierung des VMFS-basierten Datastores in VMFS-3 kann er nicht zurück in VMFS-2 konvertiert werden.
- Damit das Upgrade des Dateisystems VMFS-2 möglich ist, sollte die Dateiblockgröße nicht über 8 MB hinausgehen.

Aktualisierung von VMFS-2 in VMFS-3

1 Melden Sie sich am VMware VI Client an und wählen Sie einen Server aus dem Inventar aus.

2 Klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Speicher (SCSI, SAN und NFS)**.

3 Klicken Sie auf den Datastore, der das VMFS-2-Format verwendet.

4 Klicken Sie auf **Upgrade to VMFS-3** (Auf VMFS-3 aktualisieren).

Namensänderung von Datastores

Sie können den Namen eines bestehenden VMFS-basierten Datastores ändern.

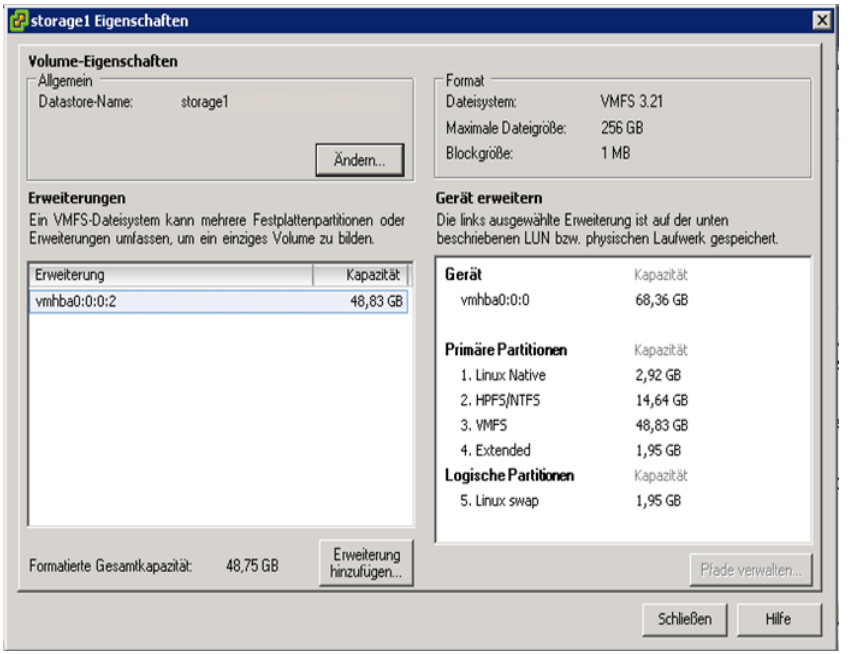
Bearbeiten des Datastore-Namens

1 Melden Sie sich am VMware VI Client an und wählen Sie einen Server aus dem Inventar aus.

2 Klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Speicher (SCSI, SAN und NFS)**.

3 Wählen Sie den Datastore aus, dessen Namen Sie bearbeiten möchten, und klicken Sie auf den **Eigenschaften**-Link.

Das Dialogfeld **Volume-Eigenschaften** wird angezeigt.



4 Klicken Sie unter **Allgemein** auf **Ändern**.

Das Dialogfeld **Eigenschaften** wird geöffnet.

5 Geben Sie den neuen Datastore-Namen ein und klicken Sie auf **OK**.

Erweiterung von Datastores

Sie können einen Datastore im VMFS-Format erweitern, indem Sie eine Festplattenpartition als Erweiterung einbinden. Der Datastore kann sich über 32 physische Speichererweiterungen erstrecken.

Sie können die neuen Erweiterungen für den Datastore dynamisch erstellen, wenn es erforderlich ist, neue virtuelle Maschinen auf diesem Datastore zu erstellen oder wenn die virtuellen Maschinen, die auf diesem Datastore ausgeführt werden, zusätzlichen Speicherplatz erfordern.

Hinzufügen von Erweiterungen zu einem Datastore

1 Melden Sie sich am VI Client an und wählen Sie einen Server aus dem Inventar aus.

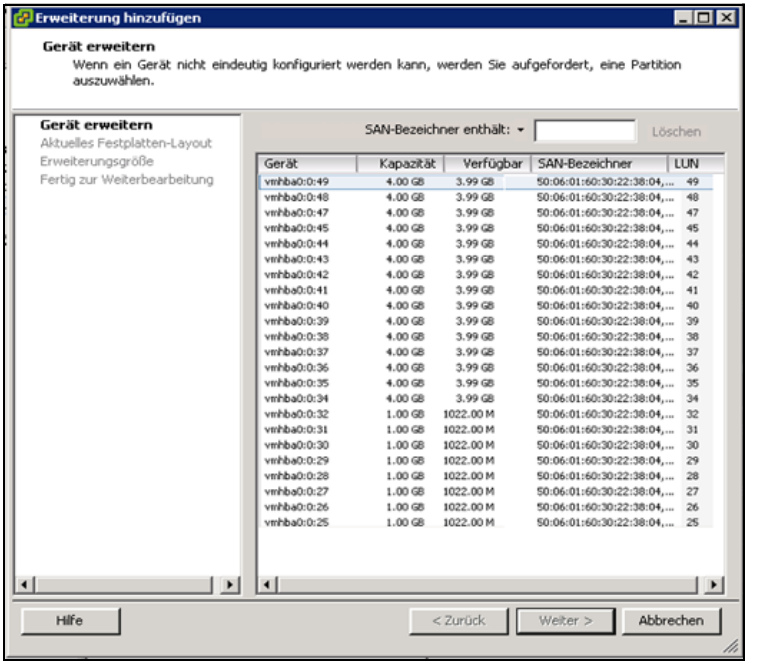
2 Klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Speicher (SCSI, SAN und NFS)**.

3 Wählen Sie den Datastore aus, den Sie erweitern möchten, und klicken Sie auf den **Eigenschaften**-Link.

Das Dialogfeld **Volume-Eigenschaften** wird angezeigt.

4 Klicken Sie unter **Erweiterungen** auf **Erweiterung hinzufügen**.

Der **Assistent zum Hinzufügen von Erweiterungen** wird geöffnet.



5 Wählen Sie die Festplatte aus, die Sie als neue Erweiterung hinzufügen möchten, und klicken Sie auf **Weiter**.

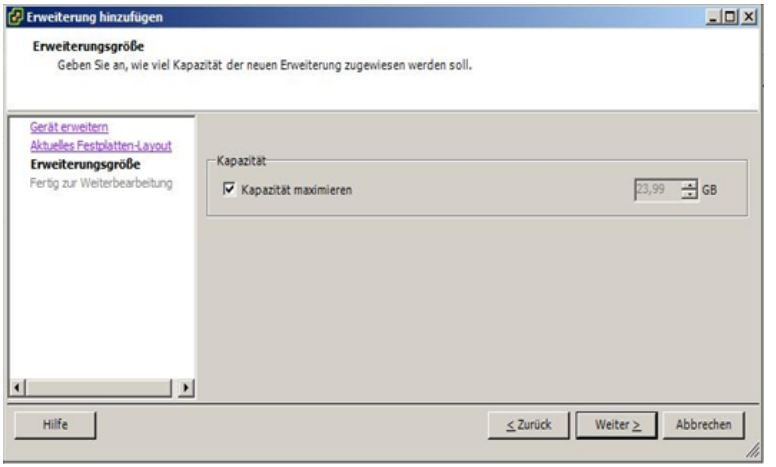
Das **Aktuelle Festplatten-Layout** wird angezeigt.

6 Überprüfen Sie das aktuelle Festplatten-Layout, die Sie für die Erweiterung verwenden möchten, um sicherzustellen, dass die Festplatte keine wichtigen Daten enthält.

HINWEIS Wenn die Festplatte oder Partition, die Sie hinzufügen möchten, vorher formatiert gewesen war, wird sie neu formatiert, wodurch alle Dateisysteme und die darin enthaltenen Daten verloren gehen.

7 Klicken Sie auf **Weiter**.

Die Seite **Erweiterungsgröße** wird angezeigt.



8 Geben Sie die Kapazität der Erweiterung an.

Standardmäßig wird der gesamte freie Speicherplatz des Speichergerätes angeboten.

9 Klicken Sie auf **Weiter**.

Das Dialogfeld **Fertig stellen** wird angezeigt.

10 Überprüfen Sie das vorgeschlagene Layout der Erweiterung und die neue Konfiguration des Datastores und klicken Sie dann auf **Fertig stellen**.

Verwalten von Pfaden für Fibre-Channel und iSCSI

ESX Server unterstützt Multipathing, um eine dauerhafte Verbindung zwischen der Server-Maschine und dem Speicher-Device für den Fall eines Ausfalls eines HBAs, eines Switches, eines Speicherprozessors (SP) oder eines Kabels aufrecht zu erhalten. Bei Multipathing-Unterstützung sind keine speziellen Failover-Treiber erforderlich.

Um Pfad-Switching zu unterstützen, verfügt der Server in der Regel über einen oder mehrere HBAs, über die der Speicher-Array unter Verwendung von einem oder mehreren Switches erreicht werden kann. Alternativ kann die Konfiguration auch einen HBA und zwei Speicherprozessoren aufweisen, sodass der HBA einen anderen Pfad verwenden kann, um auf den Festplatten-Array zuzugreifen.

Standardmäßig verwenden ESX Server-Systeme nur einen Pfad von einem Host zu einer bestimmten LUN zu einer bestimmten Zeit. Wenn der durch das ESX Server-System verwendete Pfad ausfällt, wählt der Server einen anderen verfügbaren Pfad

aus. Der Prozess der Erkennung eines ausgefallenen Pfads und der Wechsel auf einen anderen Pfad wird als Pfad-Failover bezeichnet. Ein Pfad fällt aus, wenn einer der Komponenten–HBA, Kabel, Switch-Port oder Speicherprozessor–gemeinsam mit dem Pfad ausfällt.

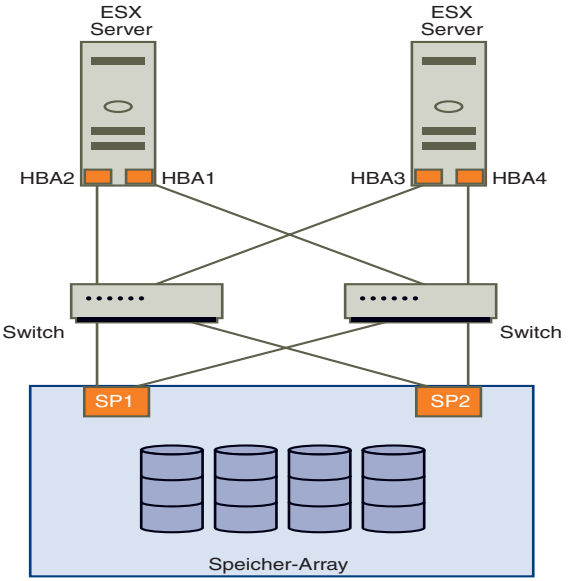


Abbildung 7-1. Multipathing

Die Abbildung Abbildung 7-1 zeigt, dass jeder Server über mehrere Pfade mit dem Speicher-Device verbunden ist. Wenn zum Beispiel HBA1 oder die Verbindung zwischen HBA1 und dem Switch ausfällt, übernimmt HBA2 und stellt eine Verbindung zwischen dem Server und dem Switch zur Verfügung. Der Prozess, in dem ein HBA für einen anderen HBA einspringt, wird als HBA-Failover bezeichnet.

Analog dazu übernimmt SP2 bei einem Ausfall von SP1 oder der Verbindung zwischen SP1 und dem Switch und stellt eine Verbindung zwischen dem Switch und dem Speichergerät zur Verfügung. Dieser Vorgang wird SP-Failover genannt. VMware ESX Server unterstützt über die Multipathing-Funktion sowohl HBA- als auch SP-Failover.

Weitere Informationen über Multipathing finden Sie im *Handbuch zur SAN-Konfiguration*.

In den folgenden Abschnitten erhalten Sie Informationen über das Verwalten von Pfaden.

- „Anzeige des aktiven Multipathing-Status“ auf Seite 145
- „Aktive Pfade“ auf Seite 146
- „Einrichten der Multipathing-Policys für LUNs“ auf Seite 147
- „Deaktivieren und Aktivieren von Pfaden“ auf Seite 148
- „Einrichten des bevorzugten Pfads (Nur feste Pfadkonventionen)“ auf Seite 149

Anzeige des aktiven Multipathing-Status

Verwenden Sie den Virtual Infrastructure Client zum Anzeigen des aktuellen Multipathing-Status.

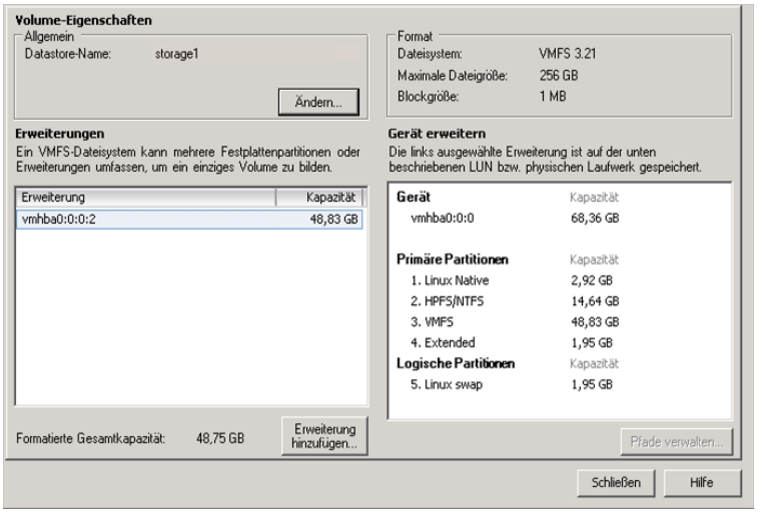
So zeigen Sie den aktuellen Multipathing-Status an

1 Melden Sie sich am VMware VI Client an und wählen Sie einen Server aus dem Inventar aus.

2 Klicken Sie auf die Registerkarte **Konfiguration** und klicken Sie unter Hardware auf **Speicher (SCSI, SAN und NFS)**.

3 Wählen Sie aus dem Verzeichnis der konfigurierten Datastores den Datastore aus, dessen Pfade Sie anzeigen oder konfigurieren möchten, und klicken Sie auf **Eigenschaften**.

Das Dialogfeld **Volume-Eigenschaften** für diesen Datastore wird geöffnet.

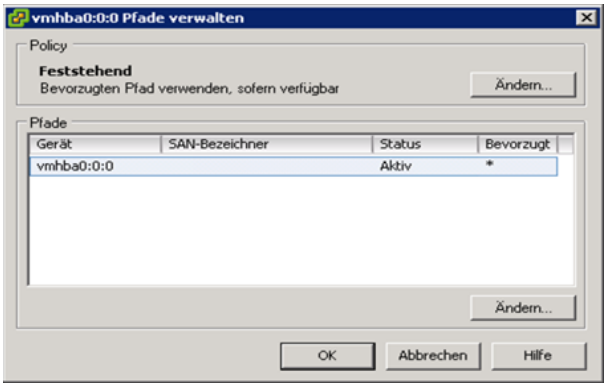


Das Fenster **Geräteerweiterung** enthält Informationen über den Status jedes einzelnen Pfads zum Speicher-Device. Die folgenden Pfadinformationen werden angezeigt:

- **Aktiv** – Der Pfad ist aktiv und ist der aktuell verwendete Pfad für die Übermittlung von Daten.
- **Deaktiviert** – Der Pfad wurde deaktiviert; Daten können nicht übertragen werden.
- **Betriebsbereit** – Der Pfad ist aktiv, er wird jedoch derzeit nicht zum Übertragen von Daten verwendet.
- **Ausgefallen** – Die Software kann über diesen Pfad keine Verbindung mit der Festplatte herstellen.

4 Klicken Sie auf **Pfade verwalten**, um den Assistenten zum **Verwalten von Pfaden** zu öffnen.

Wenn Sie die Pfadkonventionen **Feststehend** verwenden, können Sie erkennen, welcher Pfad der bevorzugte Pfad ist. Der bevorzugte Pfad ist mit einem Asterisk-Zeichen (*) in der vierten Spalte gekennzeichnet.



Sie können den Assistenten zum **Verwalten von Pfaden** verwenden, um die Pfade zu aktivieren oder zu deaktivieren, die Multipathing-Policy zu konfigurieren oder um den bevorzugten Pfad anzugeben.

Folgen Sie den folgenden Vorgehensweisen:

- „So richten Sie die Multipathing-Policy ein“ auf Seite 147
- „So deaktivieren Sie einen Pfad“ auf Seite 149
- „So aktivieren Sie einen Pfad“ auf Seite 149
- „So richten Sie den bevorzugten Pfad ein“ auf Seite 150

Aktive Pfade

ESX Server führt in der Regel kein I/O-Lastausgleich über die Pfade eines bestimmten Speicher-Devices durch. Zu einem bestimmten Zeitpunkt wird nur ein Einzelpfad zu verwendet, um I/O an ein Speicher-Device auszugeben. Der Pfad wird als aktiver Pfad bezeichnet.

- Wenn die Pfadkonventionen eines Speicher-Devices auf **Feststehend** gesetzt wurde, wählt ESX Server den Pfad, der als **Bevorzugt** gekennzeichnet ist, als den aktiven Pfad aus.

  Wenn der bevorzugte Pfad deaktiviert wurde oder auf andere Weise nicht verfügbar ist, verwendet das ESX Server-System einen alternativen aktiven Pfad als aktiven Pfad.

- Wenn die Pfadkonventionen eines Speicher-Devices auf **Zuletzt verwendet** stehen, wählt der ESX Server-Host einen aktiven Pfad für das Speicher-Device aus, um Pfad-Thrashing zu verhindern. Die Bezeichnung „Bevorzugter Pfad“ wird dabei ignoriert.

Einrichten der Multipathing-Policys für LUNs

Die folgenden Multipathing-Policys werden derzeit unterstützt:

- **Feststehend** – Der ESX Server-Host verwendet immer den bevorzugten Pfad zur Festplatte, wenn dieser Pfad verfügbar ist. Wenn nicht über den bevorzugten Pfad auf die Festplatte zugegriffen werden kann, werden die anderen Pfade probiert. **Dies** ist die Standard-Policy für Aktiv/Aktiv-Speichergeräte.
- **Zuletzt verwendet** – Der ESX Server-Host verwendet immer den zuletzt verwendeten Pfad zur Festplatte, und zwar so lange, bis der Pfad nicht mehr verfügbar ist. Dies bedeutet, dass der ESX Server-Host nicht automatisch zum bevorzugten Pfad zurückkehrt. **Zuletzt verwendet** ist die Standard-Policy für aktive/passive Speicher-Devices und wird für diese Geräte benötigt.

Der ESX Server-Host stellt die Multipathing-Policy automatisch und entsprechend des erkannten Array-Modells ein. Wenn der erkannte Array nicht unterstützt wird, wird er als aktiv/aktiv betrachtet. Im *Handbuch der SAN-Kompatibilität* finden Sie eine Liste der unterstützten Arrays.

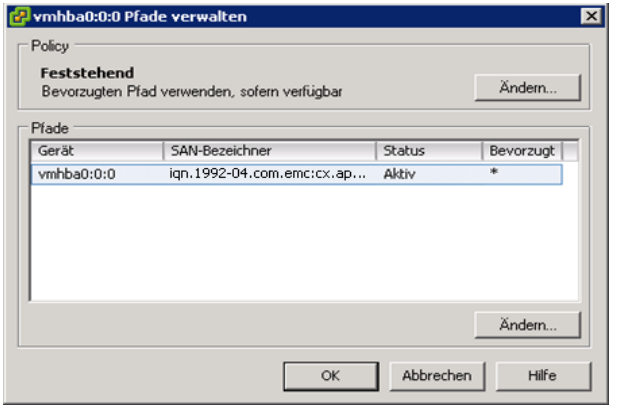
HINWEIS Es wird davon abgeraten, die Einstellung **Zuletzt verwendet** manuell in **Feststehend** zu ändern. Das System stellt diese Policy für die Arrays ein, für die diese Einstellung erforderlich ist.

So richten Sie die Multipathing-Policy ein

1 Öffnen Sie den Assistenten zum **Verwalten von Pfaden**, indem Sie die unter „So zeigen Sie den aktuellen Multipathing-Status an“ auf Seite 145 aufgeführten Schritte ausführen.

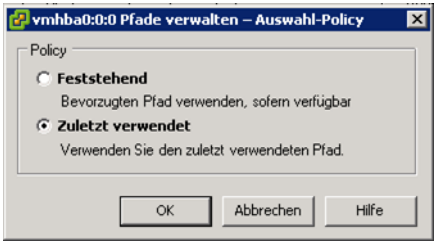
Wenn Sie Pfade für Raw-Device-Maps verwalten, finden Sie weitere Informationen unter „Pfade verwalten“ auf Seite 163.

Der Assistent zum **Pfade verwalten** enthält eine Liste mit verschiedenen Pfaden zur Festplatte sowie die Multipathing-Policy für die Festplatte und den Verbindungsstatus für jeden einzelnen Pfad. Es zeigt außerdem den bevorzugten Pfad zu der Festplatte an.



2 Klicken Sie unter **Policy** auf **Ändern**.

Das Dialogfeld **Policy auswählen** wird angezeigt.



3 Wählen Sie eine Option aus:

- **Feststehend**
- **Zuletzt verwendet**

4 Klicken Sie auf **OK** und dann auf **Schließen**, um die Einstellungen zu speichern und zum Dialogfeld **Konfiguration** zurückzukehren.

HINWEIS Bei aktiven/passiven Speicher-Devices wird die Einstellung **Zuletzt verwendet** dringend empfohlen.

Deaktivieren und Aktivieren von Pfaden

Falls es erforderlich ist, Pfade aus Wartungs- oder anderen Gründen vorübergehend zu deaktivieren, können Sie die erforderlichen Schritte über den Virtual Infrastructure Client ausführen.

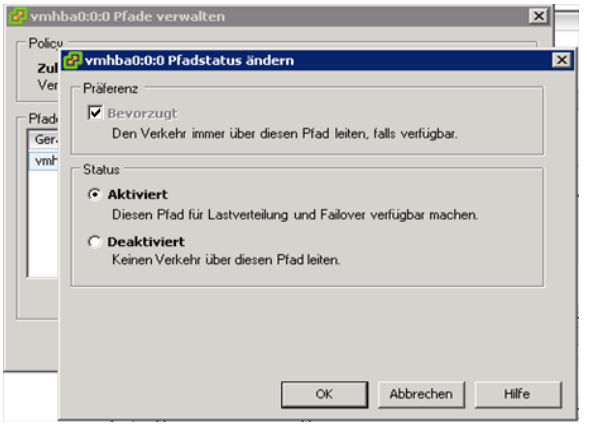
So deaktivieren Sie einen Pfad

1 Öffnen Sie den Assistenten zum **Verwalten von Pfaden**, indem Sie die unter „So zeigen Sie den aktuellen Multipathing-Status an“ auf Seite 145 aufgeführten Schritte ausführen.

Wenn Sie Pfade für Raw-Device-Maps verwalten, finden Sie weitere Informationen unter „Pfade verwalten“ auf Seite 163.

Der Assistent zum **Pfade verwalten** wird angezeigt.

2 Wählen Sie unter **Pfade** den zu deaktivierenden Pfad aus und klicken Sie auf **Ändern**.



3 Wählen Sie das Optionsfeld **Deaktivieren** aus, um den Pfad zu deaktivieren.

4 Klicken Sie zweimal auf **OK**, um Ihre Änderungen zu speichern und die Dialogfelder zu schließen.

So aktivieren Sie einen Pfad

Wenn Sie einen Pfad deaktiviert haben (z.B. aus Wartungsgründen), können Sie diesen Pfad über die unter „So deaktivieren Sie einen Pfad“ auf Seite 149 beschriebenen Schritte aktivieren. Sie müssen allerdings nun das Optionsfeld **Aktivieren** anklicken.

Einrichten des bevorzugten Pfads (Nur feste Pfadkonventionen)

Wenn Sie die Pfadkonventionen auf **Feststehend** setzen, verwendet der Server immer den bevorzugten Pfad, wenn dieser verfügbar ist.

So richten Sie den bevorzugten Pfad ein

1 Öffnen Sie den Assistenten zum **Verwalten von Pfaden**, indem Sie die unter „So zeigen Sie den aktuellen Multipathing-Status an“ auf Seite 145 aufgeführten Schritte ausführen.

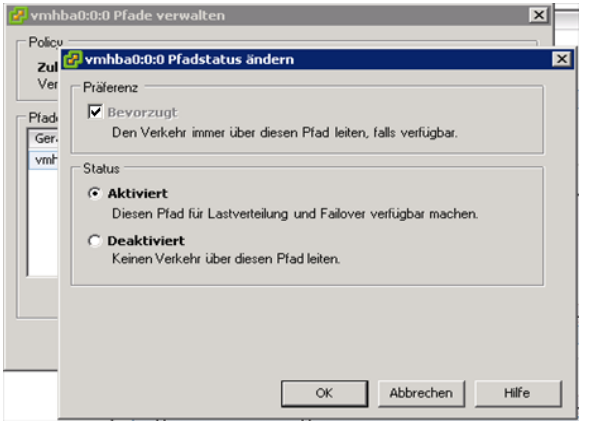
Wenn Sie Pfade für Raw-Device-Maps verwalten, finden Sie weitere Informationen unter „Pfade verwalten“ auf Seite 163.

Der Assistent zum **Pfade verwalten** wird angezeigt.

2 Wählen Sie unter „Pfade“ den Pfad aus, der der bevorzugte Pfad werden soll, und klicken Sie anschließend auf **Ändern**.

3 Klicken Sie im Bereich **Einstellungen** auf **Bevorzugt**.

Wenn die Option **Bevorzugt** nicht verfügbar ist, stellen Sie sicher, dass die **Pfadkonventionen** auf **Feststehend** gestellt sind.



4 Klicken Sie zweimal auf **OK**, um Ihre Einstellungen zu speichern und die Dialogfelder zu schließen.

Die `vmkfstools`-Befehle

Die `vmkfstools`-Befehle bieten zusätzliche Funktionen zur Erstellung von Dateien mit einer bestimmten Größe und zum Import/Export von Dateien in das und aus dem Dateisystem der Servicekonsole. Außerdem wurde `vmkfstools` zum Umgang mit großen Dateien entworfen, wodurch die Beschränkung von 2 GB, der manche Standard-Datei-Dienstprogramme unterliegen, überwunden wird.

Ein Verzeichnis der unterstützten `vmkfstools`-Befehle finden Sie unter „Verwendung von vmkfstools“ auf Seite 281.

Raw-Device-Mapping

8

Raw Device Mapping (RDM) liefert der virtuellen Maschine einen Mechanismus für den direkten Zugriff auf eine LUN auf dem physischen Speichersubsystem (nur Fibre-Channel oder iSCSI). Dieses Kapitel enthält Informationen über RDM.

HINWEIS Informationen über die Konfiguration von SANs finden Sie im *Handbuch zur SAN-Konfiguration*.

In diesem Kapitel werden folgende Themen behandelt:

- „Wissenswertes über Raw Device Mapping“ auf Seite 152
- „Raw Device Mapping-Eigenschaften“ auf Seite 156
- „Verwalten zugeordneter LUNs“ auf Seite 161

Wissenswertes über Raw Device Mapping

RDM ist eine Zuordnungsdatei in einem VMFS-Volume, die als Proxy für ein physisches Raw-Device fungiert. RDM enthält Metadaten, mit denen Plattenzugriffe auf das physische Gerät verwaltet und umgeleitet werden. Diese Datei bietet Ihnen die Vorteile des direkten Zugriffs auf das physische Gerät, während Sie gleichzeitig einige Vorteile einer virtuellen Festplatte im VMFS-Dateisystem beibehalten können. Folglich verbindet die Datei die VMFS-Verwaltungs- und Wartungsfreundlichkeit mit einem Raw-Device-Zugriff.

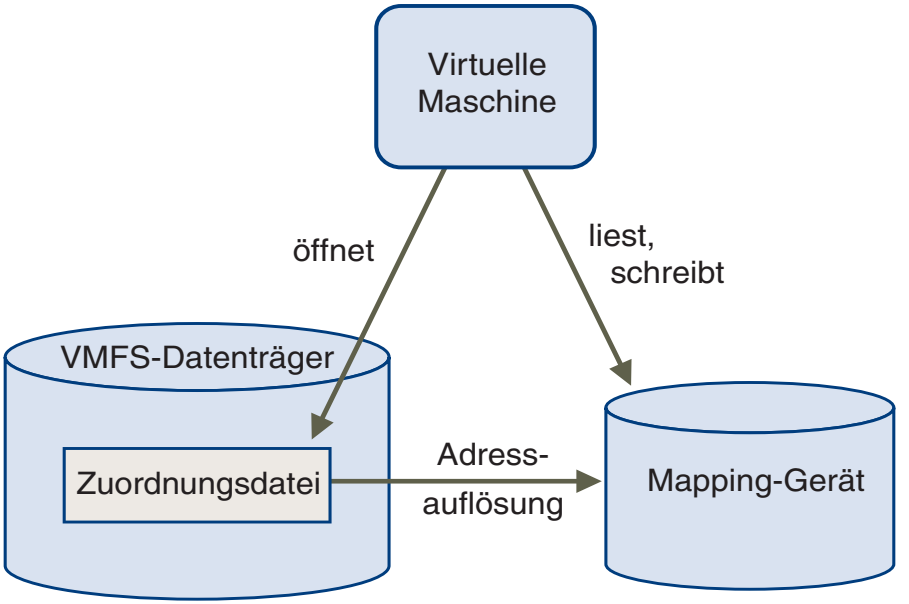


Abbildung 8-1. Raw-Device-Mapping

Obwohl VMFS für die meisten virtuellen Festplattenspeicher empfohlen wird, kann es in Einzelfällen erforderlich sein, Raw-LUNs zu verwenden.

So ist es beispielsweise in folgenden Situationen erforderlich, Raw-LUNs zusammen mit RDMs zu verwenden:

- Wenn in der virtuellen Maschine SAN-Snapshot oder andere Layer-Anwendungen ausgeführt werden. RDM unterstützt skalierbare Backup-Offloading-Systeme, die Funktionsmerkmale von SAN verwenden, besser.
- In allen MSCS-Cluster-Szenarien, die über mehrere physische Hosts verlaufen – in VM-VM-Clustern und in PC-VM-Clustern. In diesem Fall sollten Cluster-Daten und Quorumfestplatten vorzugsweise als RDMs konfiguriert werden und nicht als Dateien auf einem freigegebenen VMFS.

Stellen Sie sich die RDM-Datei als eine symbolische Verknüpfung zwischen einem VMFS-Volume und einer Raw-LUN vor (Siehe Abbildung 8-1). Die Zuordnung lässt die LUNs wie Dateien auf einem VMFS-Datenträger aussehen. In der Konfiguration der virtuellen Maschine wird auf die Zuordnungsdatei und nicht auf die Raw-LUN verwiesen. Die RDM-Datei enthält einen Verweis auf die Raw-LUN.

Mithilfe von RDMs ist Folgendes möglich:

- Migration von virtuellen Maschinen mit VMotion über Raw-LUNs.
- Hinzufügen von Raw-LUNs zu virtuellen Maschinen mithilfe des VI Clients.
- Verwendung von Dateisystemfunktionen wie verteilte Dateisperrung, Zugriffsberechtigungen und vereinfachte Namensgebung.

Für RDMs gibt es zwei Kompatibilitätsmodi:

- Mit dem Modus „Virtuelle Kompatibilität“ kann sich ein RDM genau wie eine virtuelle Festplattendatei verhalten. Dies umfasst auch die Verwendung von Snapshots.
- Mit dem Modus „Physische Kompatibilität“ kann direkt auf das SCSI-Gerät zugegriffen werden. Dies wird bei Anwendungen eingesetzt, die die Steuerung von niedrigeren Ebenen benötigen.

Begriffe

RDMs können beispielsweise wie folgt beschrieben werden: „Zuordnen eines Raw-Devices zu einem Datastore,“ „Zuordnen einer System-LUN“ oder „Zuordnen einer Festplattendatei zu einem physischen Festplatten-Volume.“ All diese Zuordnungsbegriffe beziehen sich auf RDMs.

Vorteile der Raw-Device-Mapping

RDM bietet mehrere Vorteile, aber sollte nicht in jeder Situation verwendet werden. In der Regel sind virtuelle Festplattendateien aufgrund ihrer Verwaltungs- und Wartungsfreundlichkeit dem RDM vorzuziehen. Wenn Sie jedoch Raw-Devices benötigen, müssen Sie eine RDM-Zuordnungsdatei verwenden. In der folgenden Liste sind die Vorteile von RDM zusammengefasst.

- **Benutzerfreundliche, dauerhafte Namen** – RDM ermöglicht benutzerfreundliche Namen für zugeordnete Geräte. Wenn Sie eine RDM-Zuordnung verwenden, müssen Sie nicht den Gerätenamen des Geräts verwenden. Sie verwenden stattdessen den Namen der Zuordnungsdatei, zum Beispiel:

  ```
  /vmfs/volumes/myVolume/myVMDirectory/myRawDisk.vmdk
  ```

- **Dynamische Namensauflösung** – RDM speichert eindeutige Identifikationsdaten für jedes zugeordnete Gerät. Das VMFS-Dateisystem ordnet jede RDM-Zuordnung unabhängig von Änderungen der physischen Konfiguration des Servers durch Adapter-Hardware-Änderungen, Verzeichniswechsel, Geräteverschiebungen usw. Ihrem gegenwärtigen SCSI-Gerät zu.

- **Verteilte Dateisperrung** – Die RDM-Zuordnung ermöglicht die Verwendung einer verteilten VMFS-Sperrung für Raw-SCSI-Geräte. Die verteilte Sperrung auf einer RDM-Zuordnung ermöglicht die Verwendung einer freigegebenen Raw-LUN ohne Datenverlustrisiko, wenn zwei virtuelle Maschinen auf verschiedenen Servern versuchen, auf die gleiche LUN zuzugreifen.
- **Dateizugriffsberechtigungen** – Die RDM-Zuordnung ermöglicht Dateizugriffsberechtigungen. Die Zugriffsberechtigungen der Zuordnungsdatei werden bei der Öffnung der Datei erzwungen, um den zugeordneten Datenträger zu schützen.
- **Dateisystemoperationen** – Die RDM-Zuordnung ermöglicht bei der Arbeit mit einem zugeordneten Volume die Verwendung von Dienstprogrammen des Dateisystems, wobei die Zuordnungsdatei als Proxy verwendet wird. Die meisten Vorgänge, die mit einer normalen Datei durchgeführt werden können, können auf die Zuordnungsdatei angewendet werden und werden dann auf das zugeordnete Gerät umgeleitet.
- **Snapshots** – Die RDM-Zuordnung ermöglicht die Verwendung von Snapshots virtueller Maschinen auf einem zugeordneten Volume.

HINWEIS Snapshots stehen nicht zur Verfügung, wenn die RDM-Zuordnung im Modus „Physische Kompatibilität“ verwendet wird.

- **VMotion** – Die RDM-Zuordnung ermöglicht die Migration einer virtuellen Maschine mit VMotion. Die Zuordnungsdatei arbeitet als Proxy, sodass VirtualCenter die virtuelle Maschine mit dem gleichen Mechanismus migrieren kann, der für die Migration von virtuellen Festplattendateien verwendet wird. Weitere Informationen finden Sie unter Abbildung 8-2.

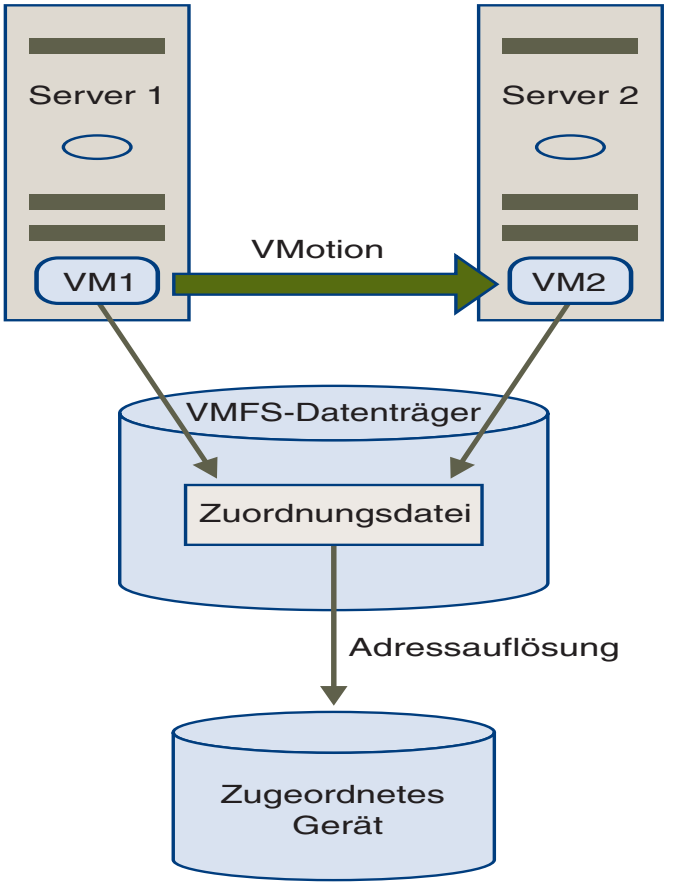


Abbildung 8-2. VMotion einer virtuellen Maschine über die Raw-Device-Mapping

- **SAN-Management-Agenten** – Die RDM-Zuordnung ermöglicht die Ausführung bestimmter SAN-Management-Agenten innerhalb der virtuellen Maschine. Außerdem kann jede Software, die Zugriff auf ein Gerät über hardwarespezifische SCSI-Befehle benötigt, in einer virtuellen Maschine ausgeführt werden. Diese Art der Software wird auch SCSI-Target-basierte Software genannt.

HINWEIS Wenn Sie SAN-Management-Agenten verwenden, müssen Sie den physischen Kompatibilitätsmodus für die RDM-Zuordnungsdatei auswählen.

VMware kooperiert mit Anbietern von Speicher-Management-Software, damit diese Software in Umgebungen wie ESX Server richtig funktioniert. Dies gilt unter anderem für folgende Anwendungen:

- SAN-Management-Software

- SRM (Speicherressourcen-Management)-Software
- Snapshot-Software
- Replikations-Software

Diese Software verwendet für RDM-Zuordnungen den Modus „Physische Kompatibilität“, damit sie direkt auf die SCSI-Geräte zugreifen kann.

Manche Management-Produkte werden besser zentral (nicht auf dem ESX Server-Computer) ausgeführt, während andere problemlos in der Servicekonsole oder in den virtuellen Maschinen funktionieren. VMware zertifiziert diese Anwendungen nicht und stellt auch keine Kompatibilitätsmatrix zur Verfügung. Wenn Sie wissen möchten, ob eine SAN-Management-Anwendung in einer ESX Server-Umgebung unterstützt wird, wenden Sie sich an den Hersteller der SAN-Management-Software.

Einschränkungen der Raw-Device-Mapping

Beachten Sie Folgendes, wenn Sie die RDM-Zuordnung verwenden möchten:

- **Nicht verfügbar für Blockgeräte und bestimmte RAID-Geräte** – Die RDM-Zuordnung (in der gegenwärtigen Implementierung) verwendet zur Identifizierung des zugeordneten Geräts eine SCSI-Seriennummer. Da Blockgeräte und bestimmte direkt angeschlossene RAID-Geräte Seriennummern nicht exportieren, können sie nicht in RDM-Zuordnungen verwendet werden.
- **Nur für Volumes in VMFS-2 und VMFS-3** – Die RDM-Zuordnung erfordert das Format VMFS-2 oder VMFS-3. Unter ESX Server 3.0 kann in das Dateisystem VMFS-2 nicht geschrieben werden. Damit darin gespeicherte Dateien verwendet werden können, müssen Sie es auf VMFS-3 aktualisieren.
- **Keine Snapshots im Modus „Physische Kompatibilität“** – Wenn Sie die RDM-Zuordnung im Modus „Physische Kompatibilität“ verwenden, können Sie für die Festplatte keine Snapshots verwenden. Im Modus „Physische Kompatibilität“ kann die virtuelle Maschine eigene Snapshots oder Spiegelungsoperationen durchführen.

  Im Modus „Virtuelle Kompatibilität“ stehen Snapshots jedoch zur Verfügung. Weitere Informationen zu den Kompatibilitätsmodi finden Sie unter„Vergleich des virtuellen und des physischen Kompatibilitätsmodus“ auf Seite 157.
- **Keine Partitionszuordnung** – Für die RDM-Zuordnung muss das zugeordnete Gerät eine vollständige LUN sein. Die Abbildung auf eine Partition wird nicht unterstützt.

Raw Device Mapping-Eigenschaften

Eine RDM-Zuordnungsdatei ist eine spezielle Datei auf einem VMFS-Volume, mit deren Hilfe die Metadaten für das zugeordnete Gerät verwaltet werden. Die Management-Software sieht die Zuordnungsdatei als normale Festplattendatei, die für normale Dateisystemoperationen zur Verfügung steht. Die virtuelle Maschine erkennt das zugeordnete Gerät aufgrund der Speicher-Virtualisierungs-Layer als virtuelles SCSI-Gerät.

Zu den wichtigsten Metadaten in der Zuordnungsdatei gehören der Speicherort des zugeordneten Gerätes (Namensauflösung) und der Sperrstatus des zugeordneten Geräts.

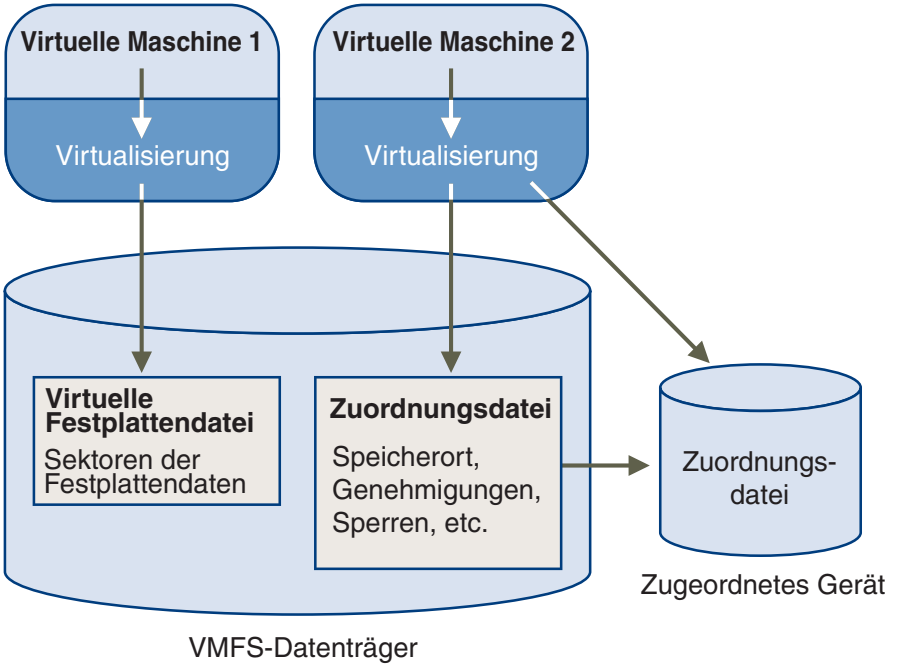


Abbildung 8-3. Metadaten der Zuordnungsdatei

Vergleich des virtuellen und des physischen Kompatibilitätsmodus

Der virtuelle Modus für eine RDM-Zuordnung legt die vollständige Virtualisierung des zugeordneten Gerätes fest. Das Gast-Betriebssystem sieht keinen Unterschied zwischen einem zugeordneten Gerät und einer virtuellen Festplattendatei auf einem VMFS-Datenträger. Die echten Hardware-Merkmale sind verborgen. Mit dem virtuellen Modus können Kunden, die Raw-Festplatten verwenden, die Vorteile von VMFS wie z. B. leistungsfähige Dateisperrung zum Datenschutz und Snapshots zur Vereinfachung von Entwicklungsprozessen nutzen. Der virtuelle Modus ist auch besser zwischen Speichern übertragbar als der physische Modus, da er das gleiche Verhalten wie virtuelle Festplattendateien aufweist.

Der physische Modus einer RDM-Zuordnung legt eine minimale SCSI-Virtualisierung des zugeordneten Geräts fest, wodurch eine optimale Flexibilität der SAN-Management-Software erreicht wird. Im physischen Modus leitet das VMkernel alle SCSI-Befehle bis auf eine Ausnahme an das Gerät weiter: Der Befehl „REPORT LUNs“ wird virtualisiert, damit das VMkernel die LUN für die entsprechende virtuelle Maschine

isolieren kann. Ansonsten sind alle physischen Charakteristika der zu Grunde liegenden Hardware sichtbar. Der physische Modus ist für die Ausführung von SAN-Management-Agenten oder anderer SCSI-basierter Software in der virtuellen Maschine bestimmt. Mit dem physischen Modus steht auch eine Clusterbildung VM-PC für kostengünstige Hochverfügbarkeit zur Verfügung.

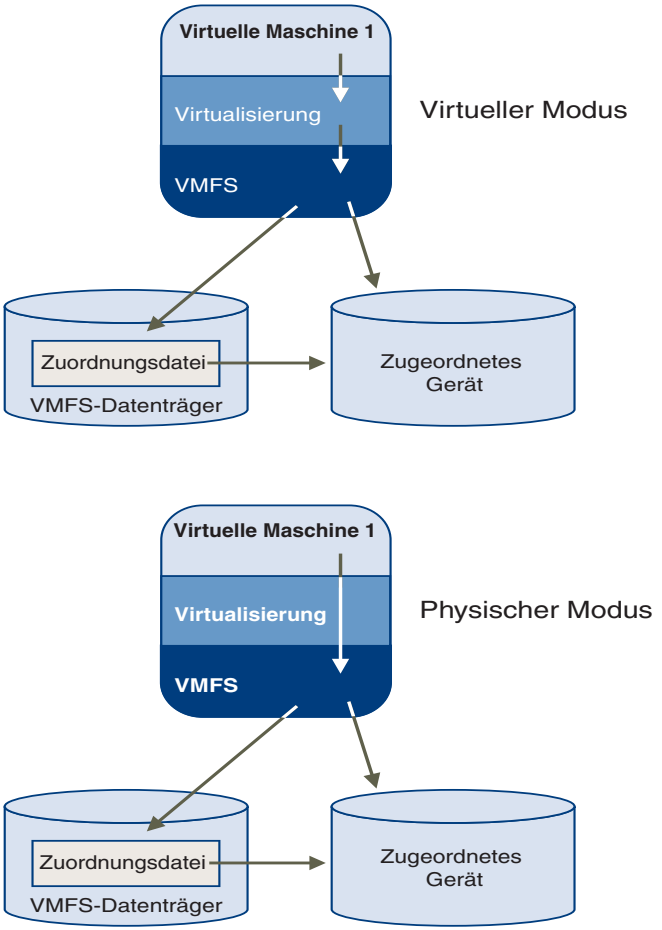


Abbildung 8-4. Die Modi „Virtuelle Kompatibilität“ und „Physische Kompatibilität“

Dynamische Namensauflösung

Mit der RDM-Zuordnung können sie einem Gerät einen dauerhaften Namen geben, indem Sie auf den Namen der Zuordnungsdatei im Unterverzeichnis `/vmfs` verweisen.

Das Beispiel in Abbildung 8-5 zeigt drei LUN. Auf LUN 1 wird über den Gerätenamen zugegriffen, der von der ersten sichtbaren LUN abhängt. LUN 2 ist ein zugeordnetes

Gerät, das von einer RDM-Zuordnungsdatei auf LUN 3 verwaltet wird. Der Zugriff auf die RDM-Zuordnungsdatei erfolgt über den feststehenden Pfadnamen im Unterverzeichnis `/vmfs`.

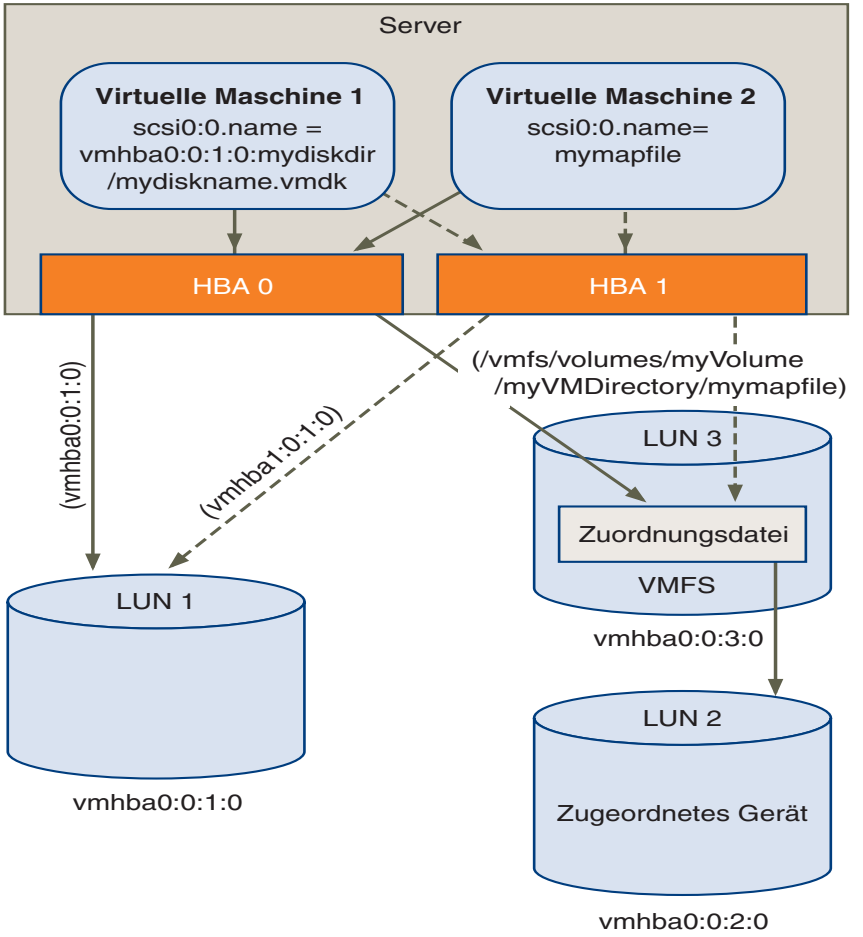


Abbildung 8-5. Beispiel für eine Namensauflösung

Alle zugeordneten LUNs werden durch VMFS eindeutig bezeichnet; die Bezeichnung wird in den internen LUN-Datenstrukturen gespeichert. Jede Änderung des SCSI-Pfads (z. B. Ausfall eines Fibre-Channel-Switches oder das Hinzufügen eines neuen Host-Bus-Adapters) kann zu einer Änderung des vmhba-Gerätenamens führen, da zum Namen auch die Pfadangabe (Ursprung, Ziel, LUN) gehört. Die dynamische Namensauflösung gleicht diese Änderungen durch die Anpassung der Datenstrukturen aus, wodurch die LUNs auf die neuen Gerätenamen umgeleitet werden.

Raw-Device-Mapping für Virtuelle-Maschinen-Cluster

Die Verwendung der RDM-Zuordnung ist für Cluster mit virtuellen Maschinen erforderlich, die zur Sicherstellung von Failover auf die gleiche Raw-LUN zugreifen müssen. Die Einrichtung ist vergleichbar mit der Einrichtung eines solchen Clusters mit Zugriff auf dieselbe virtuelle Festplattendatei; die virtuelle Festplattendatei wird dabei allerdings durch die RDM-Zuordnungsdatei ersetzt.

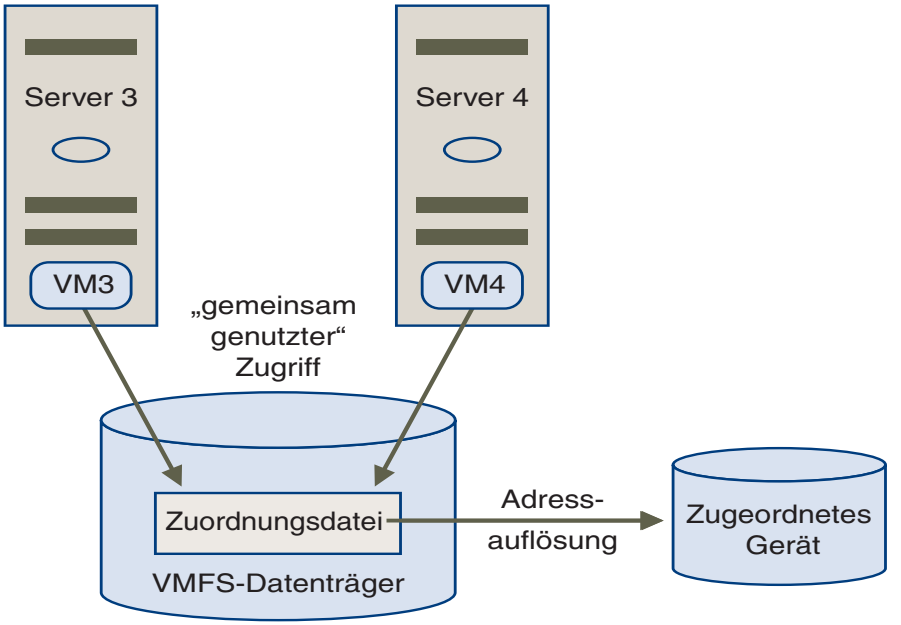


Abbildung 8-6. Zugriff aus geclusterten virtuellen Maschinen

Weitere Informationen über das Konfigurieren von Clustering finden Sie in den Handbüchern *Einrichtung des Microsoft Cluster-Dienstes* und *Handbuch zum Ressourcen-Management*.

Vergleich der Raw-Device-Mapping mit anderen Arten des SCSI-Gerätezugriffs

Um die Entscheidung zwischen den verschiedenen verfügbaren Zugriffsmodi für SCSI-Geräte zu erleichtern, gibt Tabelle 8-1 einen kurzen Vergleich der Funktionen der verschiedenen Modi.

Tabelle 8-1. Verfügbare Funktionen bei virtuellen Festplatten und Raw-Device-Mapping

ESX Server-Funktion	Virtuelle Festplattendatei	RDM - Virtueller Modus	RDM - Physischer Modus
Weitergabe von SCSI-Befehlen	Nein	Nein	Ja[1]
Unterstützung von VirtualCenter	Ja	Ja	Ja
Snapshots	Ja	Ja	Nein
Verteilte Sperrung	Ja	Ja	Ja
Clustering	Nur CIB[2]	CIB, CAB[3, 4]	Nur N+1[5]
SCSI-basierte Software	Nein	Nein	Ja

1 REPORT LUNS wird nicht weitergegeben

2 CIB = Cluster auf einem Computer

3 CAB = Cluster über mehrere Computer

4 VMware empfiehlt für CIB die Verwendung von virtuellen Festplattendateien. Verwenden Sie für CIB RDM im virtuellen Modus, wenn die CIB-Cluster als CAB-Cluster neu konfiguriert werden. Weitere Informationen über das Clustering finden Sie in den Handbüchern *Einrichtung des Microsoft Cluster-Dienstes* und *Handbuch zum Ressourcen-Management*.

5 N+1 = Cluster aus physischen Computern und virtuellen Maschinen

Verwalten zugeordneter LUNs

Zu den Werkzeugen, die für die Verwaltung zugeordneter LUNs und ihrer RDMs, bzw. Zuordnungsdateien, verfügbar sind, gehört der VI Client von VMware, das Dienstprogramm `vmkfstools` und die normalen Dateisystemdienstprogramme, die in der Servicekonsole verwendet werden.

Weitere Informationen finden Sie unter folgenden Themen:

- „Virtual Infrastructure Client (VI Client)“ auf Seite 161
- „Das vmkfstools Dienstprogramm“ auf Seite 164
- „Dateisystemfunktionen“ auf Seite 164

Virtual Infrastructure Client (VI Client)

Mithilfe des VI Client können Sie eine SAN-LUN einem Datastore zuordnen und Pfade zur zugeordneten LUN verwalten.

Weitere Informationen finden Sie in folgenden Abschnitten:

- „Zuordnen einer SAN-LUN“ auf Seite 162
- „Verwalten von Pfaden für eine zugeordnete Raw-LUN“ auf Seite 163

Zuordnen einer SAN-LUN

Wenn Sie einem VMFS-Volume eine LUN zuordnen, erstellt VirtualCenter eine Zuordnungsdatei (RDM), die auf die Raw-LUN verweist. Zwar hat die Zuordnungsdatei die Erweiterung VMDK, die Datei enthält jedoch nur beschreibende Festplatteninformationen für die LUN-Zuordnung auf dem ESX Server-System. Die eigentlichen Daten sind auf der LUN gespeichert.

So ordnen Sie eine SAN-LUN zu:

1 Melden Sie sich als Administrator oder als Besitzer der virtuellen Maschine, zu der die zugeordnete Festplatte gehören wird, an.

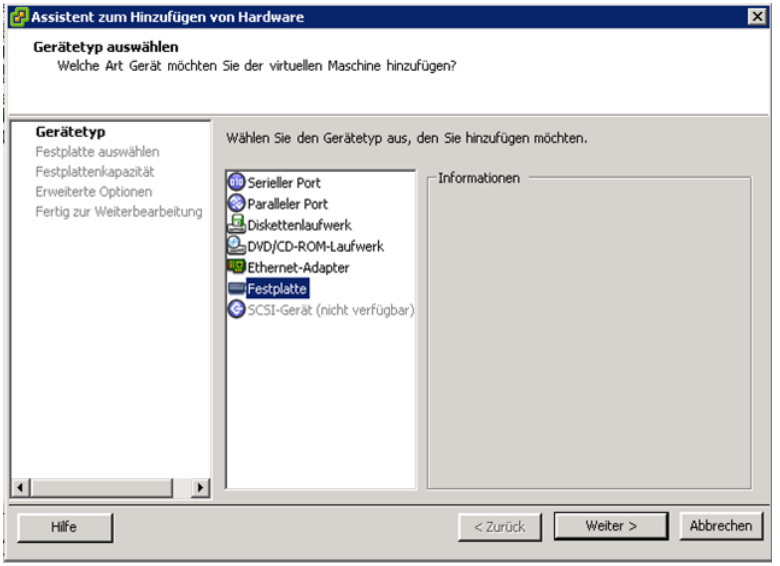
2 Wählen Sie die virtuelle Maschine aus dem Inventar aus.

3 Klicken Sie auf der Registerkarte **Übersicht** auf **Einstellungen bearbeiten**.

Das Dialogfeld Eigenschaften der virtuellen Maschinen wird geöffnet.

4 Klicken Sie auf **Hinzufügen**.

Der Assistent zum Hinzufügen von Hardware wird geöffnet.



5 Wählen Sie als Gerät, das hinzugefügt werden soll, **Festplatte** aus, und klicken Sie auf **Weiter**.

6 Wählen Sie im Fenster Festplatte auswählen **Zugeordnete SAN-LUN** aus.

7 Wählen Sie eine Raw-LUN aus der Liste der verfügbaren LUNs aus.

8 Wählen Sie einen Datastore aus, dem die Raw-LUN zugeordnet werden soll.

9 Wählen Sie **Physisch** oder **Virtuell** als Kompatibilitätsmodus aus.

In Abhängigkeit der von Ihnen getroffenen Auswahl werden in den nachfolgenden Bildschirmen unterschiedliche Optionen angeboten.

10 Auf der Seite „Erweiterte Optionen spezifizieren“ können Sie den Node des virtuellen Geräts ändern und auf **Weiter** klicken.

Die Seite „Neue virtuelle Maschine fertig zur Weiterbearbeitung“ wird angezeigt.

11 Überprüfen Sie die Optionen Ihrer neuen virtuellen Maschine und klicken Sie auf **Fertig stellen**.

Der Erstellungsvorgang einer virtuellen Maschine mit einer virtuellen Festplatte mit LUN-Zuordnung ist abgeschlossen.

Verwalten von Pfaden für eine zugeordnete Raw-LUN

Sie können den Assistenten zum Verwalten der Pfade dazu verwenden, um die Pfade Ihrer Zuordnungsdateien und zugeordneten Raw-LUNs zu verwalten.

Pfade verwalten

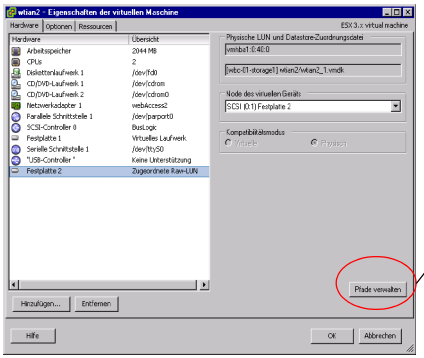
1 Melden Sie sich als Administrator oder als Besitzer der virtuellen Maschine an, zu der die zugeordnete Festplatte gehören wird.

2 Wählen Sie die virtuelle Maschine aus dem Inventar aus.

3 Klicken Sie auf der Registerkarte **Übersicht** auf **Einstellungen bearbeiten**.

Das Dialogfeld Eigenschaften der virtuellen Maschinen wird geöffnet.

4 Auf der **Hardware** Registerkarte, wählen Sie **Festplatte** aus und klicken Sie auf **Pfade verwalten**.



Pfade verwalten
Schaltfläche

Der Pfade verwalten Assistent wird geöffnet.

5 Verwenden Sie den Pfade verwalten Assistenten, um Ihre Pfade zu aktivieren oder zu deaktivieren, um die Multipath-Policy und den vorgezogenen Pfad einzustellen.

Führen Sie die folgenden Vorgehensweisen aus:

- „So richten Sie die Multipathing-Policy ein“ auf Seite 147
- „So deaktivieren Sie einen Pfad“ auf Seite 149
- „So aktivieren Sie einen Pfad“ auf Seite 149
- „So richten Sie den bevorzugten Pfad ein“ auf Seite 150

Das `vmkfstools` Dienstprogramm

In der Servicekonsole kann für viele der Operationen, die über den VI Client ausgeführt werden, das Befehlszeilendienstprogramm `vmkfstools` verwendet werden. Zu den typischen für RDM anwendbaren Operationen gehören die Befehle zur Erstellung einer Zuordnungsdatei, die Abfrage von Zuordnungsinformationen wie Name und Bezeichnung des zugeordneten Gerätes und Import und Export einer virtuellen Festplatte.

Weitere Informationen finden Sie unter „Verwendung von vmkfstools“ auf Seite 281.

Dateisystemfunktionen

Die meisten Dateisystemfunktionen, die in der Servicekonsole ausgeführt werden können, gelten auch für RDM-Zuordnungen.

`ls –l`

Der Befehl `ls` mit der Option `-l` zeigt den Dateinamen und die Zugriffsberechtigungen für die Zuordnungsdatei sowie die Größe des zugeordneten Gerätes an.

`du`

Der Befehl `du` zeigt den Speicherplatz des zugeordneten Gerätes (nicht der Zuordnungsdatei) an.

`mv`

Der Befehl `mv` benennt die Zuordnungsdatei um, beeinflusst jedoch das zugeordnete Gerät nicht.

`cp`

Mit dem Befehl `cp` können Sie den Inhalt eines zugeordneten Gerätes kopieren, umgekehrt funktioniert dieser Befehl jedoch nicht - Sie können keine virtuelle Festplattendatei auf ein zugeordnetes Gerät kopieren. Verwenden Sie dafür den `vmkfstools`-Befehl.

`dd`

Mit dem Befehl `dd` können Sie Daten vom oder auf das zugeordnete Gerät kopieren. VMware empfiehlt Ihnen jedoch aus Gründen der Effektivität, die `vmkfstools` Import- und Export-Befehle zu verwenden.

Sicherheit

Sicherheit für ESX Server-Systeme

9

Bei der Entwicklung von ESX Server war hohe Sicherheit einer der Schwerpunkte. Dieser Abschnitt bietet Ihnen eine Übersicht darüber, wie VMware die Sicherheit in der ESX Server Umgebung herstellt. Dies erfolgt insbesondere über die Sicherheitsaspekte der System-Architektur und eine Liste der zusätzlichen Sicherheitsressourcen.

Dieses Kapitel enthält folgende Abschnitte:

- „Architektur und Sicherheitsfunktionen von ESX Server“ auf Seite 168
- „Sonstige Nachschlagewerke und Informationen zur Sicherheit“ auf Seite 179

Architektur und Sicherheitsfunktionen von ESX Server

Aus Sicht der Sicherheit besteht VMware ESX Server aus vier Hauptkomponenten: der Virtualisierungs-Layer, den virtuellen Maschinen, der Servicekonsole und der virtuellen Netzwerk-Layer. Folgende Abbildung Abbildung 9-1 bietet eine Übersicht über diese Komponenten.

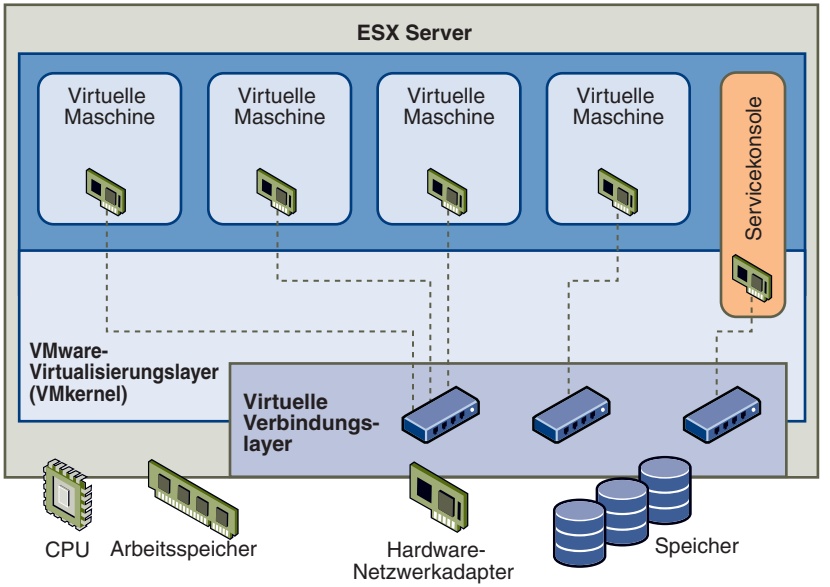


Abbildung 9-1. Architektur von ESX Server

Jede dieser Komponenten und die gesamte Architektur wurden so entworfen, dass die Sicherheit des ESX Server-Systems als Ganzes gewährleistet wird.

Sicherheit in der Virtualisierungs-Layer

Die Virtualisierungs-Layer, das sog. VMkernel ist ein Kernel, das von VMware von Grund auf für die Ausführung von virtuellen Maschinen entworfen wurde. Sie kontrolliert die Hardware, die von den ESX Server-Hosts verwendet wird, und plant die Zuweisung von Hardware-Ressourcen an die einzelnen virtuellen Maschinen. Da das VMkernel ausschließlich für die Unterstützung der virtuellen Maschinen verwendet wird, beschränkt sich die Schnittstelle zum VMkernel auf die Programmierschnittstelle, die zur Verwaltung der virtuellen Maschinen notwendig ist.

Sicherheit der virtuellen Maschinen

Virtuelle Maschinen sind die „Behälter“, in denen Anwendungen und Gastbetriebssysteme ausgeführt werden. Durch den Systemaufbau sind alle virtuellen Maschinen von VMware voneinander isoliert. Die Isolierung der virtuellen Maschine wird vom Gast-

Betriebssystem nicht wahrgenommen. Selbst ein Anwender mit Systemadministratorrechten für das Gast-Betriebssystem der virtuellen Maschine kann diese Isolierungslayer nicht durchbrechen und auf andere virtuelle Maschinen zugreifen, wenn er vom Systemadministrator von ESX Server keine entsprechenden Rechte erhalten hat.

Durch diese Isolierung können mehrere virtuelle Maschinen gleichzeitig und sicher auf der gleichen Hardware ausgeführt werden. Dabei werden sowohl Hardware-Zugriff als auch ununterbrochene Leistung garantiert. Wenn zum Beispiel ein Gast-Betriebssystem in einer virtuellen Maschine abstürzt, werden die anderen virtuellen Maschinen auf dem gleichen ESX Server-Host weiter ohne Beeinträchtigung ausgeführt. Der Absturz des Gast-Betriebssystems hat keinen Einfluss auf:

- Den uneingeschränkten Zugriff der Anwender auf die anderen virtuellen Maschinen,
- Den uneingeschränkten Zugriff der anderen virtuellen Maschinen auf die Ressourcen, die sie benötigen,
- Die Leistung der anderen virtuellen Maschinen.

Jede virtuelle Maschine ist von den anderen virtuellen Maschinen, die auf der gleichen Hardware ausgeführt werden, isoliert. Obwohl sich die virtuellen Maschinen die physischen Ressourcen wie CPU, Arbeitsspeicher und I/O-Geräte teilen, kann das Gast-Betriebssystem einer einzelnen virtuellen Maschine nur die virtuellen Geräte sehen, die ihm zur Verfügung gestellt wurden (s. Abb.Abbildung 9-2).

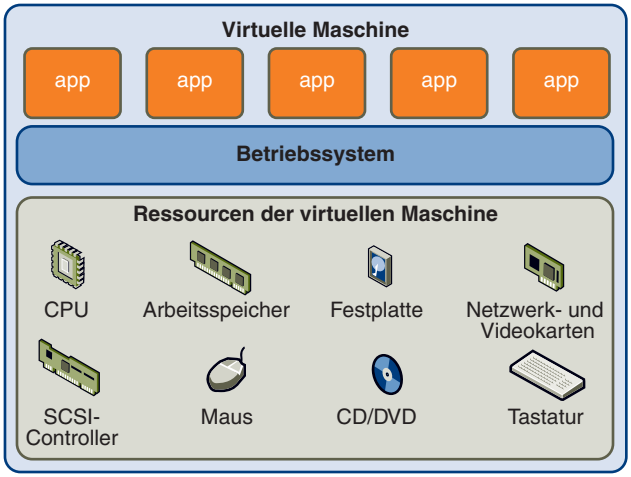


Abbildung 9-2. Isolierung virtueller Maschinen

Da das VMkernel die physischen Ressourcen vermittelt und jeder Zugriff auf die physische Hardware über das VMkernel erfolgt, können die virtuellen Maschinen diese Isolierungsstufe nicht umgehen.

So wie ein Computer mit anderen Computern in einem Netzwerk nur über eine Netzwerkkarte kommunizieren kann, kann eine virtuelle Maschine mit anderen

virtuellen Maschinen auf dem gleichen ESX Server-Host nur über einen virtuellen Switch kommunizieren. Außerdem kann die virtuelle Maschine mit einem physischen Netzwerk (einschließlich virtueller Maschinen auf anderen ESX Server-Hosts) nur über einen physischen Netzwerkadapter kommunizieren, siehe Abbildung 9-3.

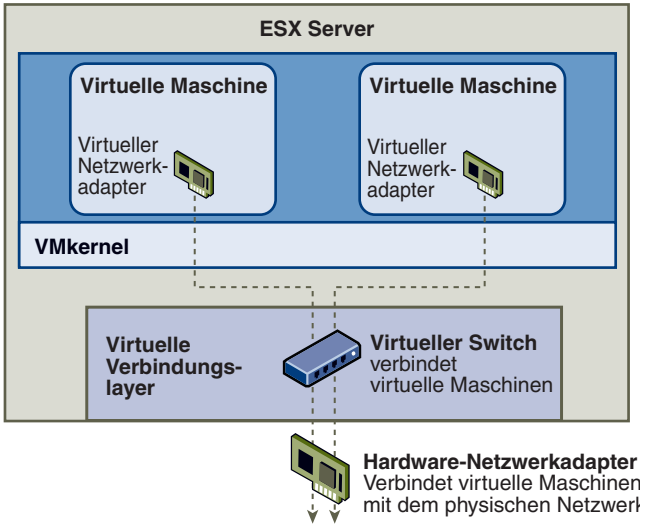


Abbildung 9-3. Virtuelle Netzwerkanbindung über virtuelle Switches

Für die Isolierung virtueller Maschinen im Netzwerk gelten folgende Regeln:

- Wenn sich eine virtuelle Maschine keinen virtuellen Switch mit anderen virtuellen Maschinen teilt, ist sie von den virtuellen Netzwerken auf dem Host vollständig getrennt.
- Wenn einer virtuellen Maschine kein physischer Netzwerkadapter zugewiesen wurde, ist die virtuelle Maschine vollständig von physischen Netzwerken getrennt.
- Wenn Sie zum Schutz einer virtuellen Maschine vor dem Netzwerk die gleichen Sicherheitsmaßnahmen wie für normale Computer verwenden (Firewalls, Anti-viren-Software usw.), ist die virtuelle Maschine genau so sicher, wie es ein Computer wäre.

Sie können die virtuelle Maschine außerdem durch die Einrichtung von Ressourcenreservierungen und -begrenzungen auf dem ESX Server-Host schützen. So können Sie zum Beispiel eine virtuelle Maschine mit den genau justierbaren Werkzeugen zur Ressourcensteuerung, die Ihnen in ESX Server zur Verfügung stehen, so konfigurieren, dass sie immer mindestens zehn Prozent der CPU-Ressourcen des ESX Server-Hosts erhält, nie jedoch mehr als zwanzig Prozent.

Ressourcenreservierungen und -begrenzungen schützen die virtuellen Maschinen vor Leistungsabfällen, wenn eine andere virtuelle Maschine versucht, zu viele Ressourcen der gemeinsam genutzten Hardware zu verwenden. Wenn zum Beispiel eine virtuelle Maschine auf dem ESX Server-Host durch eine Dienstblockade (DOS) oder verteilte Dienstblockade (DDOS) außer Gefecht gesetzt wird, verhindert eine Ressourcenbegrenzung, dass der Angriff so viele Hardware-Ressourcen einnimmt, dass die anderen virtuellen Maschinen ebenfalls betroffen werden. Ebenso stellt eine Ressourcenreservierung für jede virtuelle Maschine sicher, dass bei hohen Ressourcen-Anforderungen durch den DOS-Angriff alle anderen virtuellen Maschinen immer noch über genügend Kapazitäten verfügen.

Standardmäßig schreibt der ESX Server eine Art der Ressourcen-Reservierung vor, indem er einen Verteilungsalgorithmus verwendet, der die verfügbaren Host-Ressourcen zu gleichen Teilen auf die virtuellen Maschinen verteilt und gleichzeitig einen bestimmten Prozentsatz der Ressourcen für einen Einsatz durch andere System-Komponenten, wie z. B. die Servicekonsole bereithält. Dieses Standardverhalten bietet einen natürlichen Schutz gegen DOS- und DDOS-Angriffe. Geben Sie die spezifischen Ressourcen-Reservierungen und Grenzwerte individuell ein, wenn Sie das Standardverhalten auf Ihre Bedürfnisse so zuschneiden wollen, dass die Verteilung über die gesamte Konfiguration der virtuellen Maschine nicht einheitlich ist. Eine Abhandlung zur Verwaltung der Ressourcenzuweisung für virtuelle Maschinen finden Sie im *Handbuch zum Ressourcen-Management*.

Sicherheit über die Servicekonsole

Die Servicekonsole von ESX Server 3.0 ist eine eingeschränkte Linux-Version, die auf Red Hat Enterprise Linux 3, Aktualisierung 6 (RHEL 3 U6) beruht. Die Servicekonsole stellt eine Ausführungsumgebung für die Überwachung und Verwaltung des gesamten ESX Server-Hosts zur Verfügung.

Wenn die Servicekonsole auf bestimmte Weise beeinträchtigt wird, ist auch die von ihr gesteuerte virtuelle Maschine gefährdet. Um das Risiko eines Angriffs über die Servicekonsole zu minimieren, wird die Servicekonsole von VMware durch eine Firewall geschützt. Weitere Informationen zu dieser Firewall finden Sie unter „Konfiguration der Servicekonsolen-Firewall“ auf Seite 240.

Neben der Implementierung der Firewall der Servicekonsole verringert VMware die Risiken für die Servicekonsole auf folgende Weise:

- ESX Server verfügt nur über Dienste, die zur Verwaltung seiner Funktionen unabdingbar sind; die Servicekonsole beschränkt sich auf die Funktionen, die zum Betrieb von ESX Server notwendig sind.
- Die Standardeinstellung für die Sicherheit von ESX Server wird bei der Installation auf „hoch“ gesetzt, d. h. alle nach außen gerichteten Ports werden geschlossen und die wenigen freigegebenen, nach innen gerichteten Ports sind die Ports, die für die Kommunikation mit Clients wie dem VMware VI Client notwendig sind. VMware empfiehlt die Beibehaltung dieser Sicherheitsebene, wenn die Servicekonsole nicht an ein vertrauenswürdiges Netzwerk angeschlossen ist.

- Standardmäßig sind alle Ports, die nicht spezifisch für den Management-Zugriff auf die Servicekonsole notwendig sind, geschlossen. Wenn Sie zusätzliche Dienste benötigen, müssen Sie die jeweiligen Ports freigeben.
- Standardmäßig wird der gesamte Datenverkehr zwischen Clients über SSL verschlüsselt. Die SSL-Verbindung verwendet 256-Bit-AES-Blockverschlüsselung und 1024-Bit-RSA-Schlüsselverschlüsselung.
- Der Tomcat Web-Dienst, der intern von ESX Server zum Zugriff auf die Servicekonsole über Webclients wie VMware Virtual Infrastructure Web Access verwendet wird, wurde so angepasst, dass er nur die für die Verwaltung und Überwachung über einen Webclient notwendigen Funktionen ausführt. Daher ist ESX Server nicht von den Sicherheitslücken betroffen, die für Tomcat in weiter gefassten Anwendungsbereichen gemeldet wurden.
- VMware überwacht alle Sicherheitswarnungen, die die Sicherheit der Servicekonsole beeinflussen können, und veröffentlicht ggf. Sicherheitspatches. Gleiches gilt auch für andere Sicherheitslücken, die ESX Server-Hosts gefährden könnten. VMware veröffentlicht Sicherheits-Patches für RHEL 3 U6 und höher sobald sie zur Verfügung stehen.
- Unsichere Dienste, wie z. B. FTP und Telnet sind nicht installiert und die Ports für diese Dienste sind standardmäßig geschlossen. Da sicherere Dienste wie z. B. SSH und SFTP leicht verfügbar sind, sollten Sie stets auf einen Einsatz der unsicheren Dienste zugunsten der sichereren Alternativen unterlassen. Wenn Sie die unsicheren Dienste verwenden müssen und für die Servicekonsole einen ausreichenden Schutz hergestellt haben, müssen Sie entsprechend deren Ports öffnen, um sie zu unterstützen.
- Die Zahl der Anwendungen, die die Kennzeichen `setuid` oder `setgid` verwenden, wurde minimiert. Sie können alle `setuid`- oder `setgid`-Anwendungen, die für den Betrieb von ESX Server optional sind, deaktivieren. Weitere Informationen zu notwendigen und optionalen `setuid`- und `setgid`-Anwendungen finden Sie unter „Setuid- und setgid-Anwendungen“ auf Seite 252.

Genauere Erläuterungen zu diesen Sicherheitsmaßnahmen und anderen Sicherheitsempfehlungen für die Servicekonsole finden Sie unter „Sicherheit der Servicekonsole“ auf Seite 237.

Sie können zwar bestimmte Programme, die für RHEL 3 U6 entwickelt wurden, in der Servicekonsole installieren und ausführen, dies kann jedoch zu ernsthaften Sicherheitslücken führen und wird daher nur unterstützt, wenn VMware dies ausdrücklich anführt. Wenn eine Sicherheitslücke in der unterstützten Konfiguration erkannt wird, informiert VMware alle Kunden mit geltenden Support- und Wartungsverträgen und stellt alle notwendigen Patches zur Verfügung.

HINWEIS Bestimmte Sicherheitsmeldungen von Red Hat betreffen die ESX Server-Umgebung nicht. In diesem Fall veröffentlicht VMware keine Warnungen oder Patches.

Weitere Informationen zu den VMware Policys für Sicherheitspatches für unterstützte Programme sowie die Policys für nicht unterstützte Software finden Sie unter „Sonstige Nachschlagewerke und Informationen zur Sicherheit“ auf Seite 179.

Sicherheit in der virtuellen Netzwerk-Layer

Die virtuelle Netzwerk-Layer besteht aus den virtuellen Netzwerkgeräten, über die die virtuellen Maschinen und die Schnittstelle der Servicekonsole mit dem Rest des Netzwerkes kommunizieren. ESX Server verwendet zur Kommunikation zwischen den virtuellen Maschinen und ihren Anwendern die Konnektivitäts-Layer. Außerdem verwenden ESX Server-Hosts diese Layer zur Kommunikation mit iSCSI-SANs, NAS-Speicher usw. Zur Konnektivitäts-Layer gehören virtuelle Netzwerkadapter und virtuelle Switches.

Die Methoden, die Sie zur Absicherung eines Netzwerkes von virtuellen Maschinen verwenden, hängen unter anderem davon ab, welches Gast-Betriebssystem installiert wurde und ob die virtuellen Maschinen in einer sicheren Umgebung betrieben werden. Virtuelle Switches bieten einen hohen Grad an Sicherheit, wenn sie in Verbindung mit anderen üblichen Sicherheitsmaßnahmen wie z. B. Firewalls verwendet werden. ESX Server unterstützt auch VLANs nach IEEE 802.1q, die zum weiteren Schutz des Netzwerkes der virtuellen Maschinen, der Servicekonsole oder der Speicherkonfiguration verwendet werden können. Mit VLANs können Sie ein physisches Netzwerk in Segmente aufteilen, sodass zwei Computer im gleichen physischen Netzwerk nur dann Pakete untereinander versenden können, wenn sie sich im gleichen VLAN befinden.

In den folgenden Beispielen wird ein Eindruck davon vermittelt, wie Sie virtuelle Switches dazu verwenden können, um Sicherheitsmaßnahmen wie DMZs zu implementieren und virtuelle Maschinen in verschiedenen Netzwerken auf dem gleichen ESX Server-Host zu konfigurieren.

HINWEIS Eine eingehende Abhandlung darüber, wie virtuelle Switches und VLANs zum Schutz des Netzwerks der virtuellen Maschinen beitragen können, sowie Sicherheitsempfehlungen für Netzwerke virtueller Maschinen finden Sie unter „Absicherung virtueller Maschinen durch VLANs“ auf Seite 194.

Beispiel: Erstellung einer Netzwerk-DMZ auf einem ESX Server-Host

Ein Beispiel für die Anwendung der ESX Server-Isolierung und von virtuellen Netzwerkfunktionen zur Umgebungsabsicherung ist die Einrichtung einer entmilitarisierten Zone (DMZ) auf einem einzigen ESX Server-Host, wie in Abbildung 9-4 dargestellt.

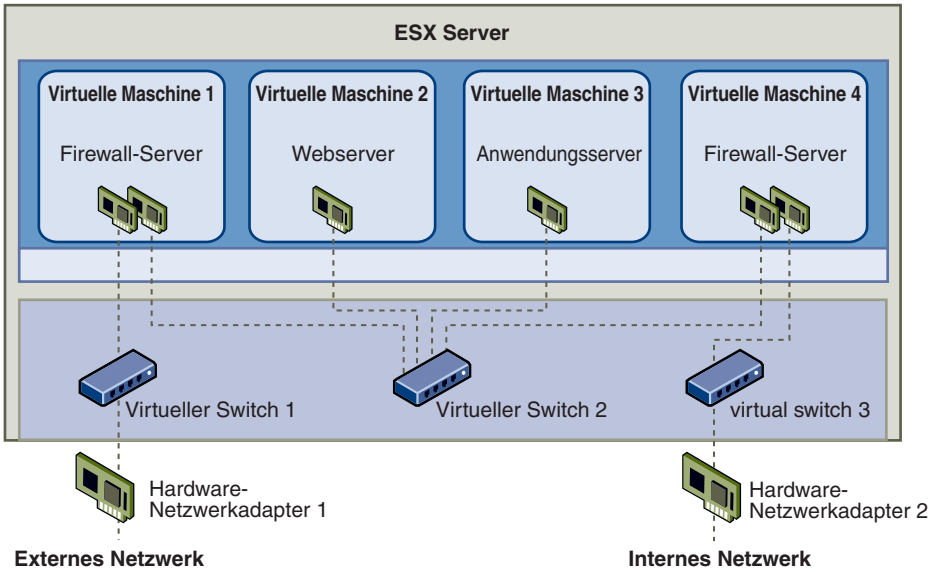


Abbildung 9-4. DMZ auf einem ESX Server-Host

Diese Konfiguration umfasst vier virtuelle Maschinen, die so konfiguriert wurden, dass sie eine virtuelle DMZ auf dem *virtuellen Switch 2* bilden. Die *virtuelle Maschine 1* und die *virtuelle Maschine 4* führen Firewalls aus und sind über virtuelle Switches an virtuelle Adapter angeschlossen. Diese beiden Maschinen verfügen über Multihoming. Auf der *virtuellen Maschine 2* wird ein Web-Server ausgeführt, auf der *virtuellen Maschine 3* ein Anwendungs-Server. Diese beiden Maschinen verfügen über Singlehoming.

Der Web-Server und der Anwendungs-Server befinden sich in der DMZ zwischen den zwei Firewalls. Die Verbindung zwischen diesen Elementen ist der *virtuelle Switch 2*, der die Firewalls mit den Servern verbindet. Dieser Switch ist nicht direkt mit Elementen außerhalb der DMZ verbunden und wird durch die beiden Firewalls vom externen Datenverkehr abgeschirmt.

Während des Betriebs der DMZ betritt externer Datenverkehr aus dem Internet die *virtuelle Maschine 1* über den *Hardware-Netzwerkadapter 1* (weitergeleitet vom *virtuellen Switch 1*) und wird von der auf dieser virtuellen Maschine installierten Firewall überprüft. Wenn die Firewall den Datenverkehr autorisiert, wird er an den virtuellen Switch in der DMZ, den *virtuellen Switch 2*, weitergeleitet. Da der Web-Server und der Anwendungs-Server ebenfalls an diesen Switch angeschlossen sind, können sie die externen Anfragen bearbeiten.

Der *virtuelle Switch 2* ist auch an die *virtuelle Maschine 4* angeschlossen. Auf dieser virtuellen Maschine schirmt eine Firewall die DMZ vom internen Firmennetzwerk ab. Diese Firewall filtert Pakete vom Web-Server und vom Anwendungs-Server. Wenn ein Paket überprüft wurde, wird es über den *virtuellen Switch 3* an den *Hardware- Netzwerkadapter 2* weitergeleitet. Der *Hardware-Netzwerkadapter 2* ist an das interne Firmennetzwerk angeschlossen.

Bei der Implementierung einer DMZ auf einem einzigen ESX Server können Sie relativ einfache Firewalls verwenden. Obwohl eine virtuelle Maschine in dieser Konfiguration keine direkte Kontrolle über eine andere virtuelle Maschine ausüben oder auf ihren Speicher zugreifen kann, sind die virtuellen Maschinen dennoch über ein virtuelles Netzwerk verbunden. Dieses Netzwerk kann für die Verbreitung von Viren oder für andere Angriffe missbraucht werden. Virtuelle Maschinen in der DMZ sind genau so sicher oder unsicher wie getrennte physische Computer im gleichen Netzwerk.

Beispiel: Erstellung mehrerer Netzwerke auf einem ESX Server-Host

Das ESX Server-System wurde so entworfen, dass Sie bestimmte Gruppen von virtuellen Maschinen an das interne Netzwerk anbinden können, andere an das externe Netzwerk, und wiederum andere an beide Netzwerke – und zwar alles im Rahmen des gleichen ESX Server-Hosts. Diese Fähigkeit basiert auf der grundlegenden Isolierung von virtuellen Maschinen im Zusammenspiel mit der gut geplanten Verwendung von Funktionen zur virtuellen Vernetzung, wie in Abbildung 9-5 dargestellt.

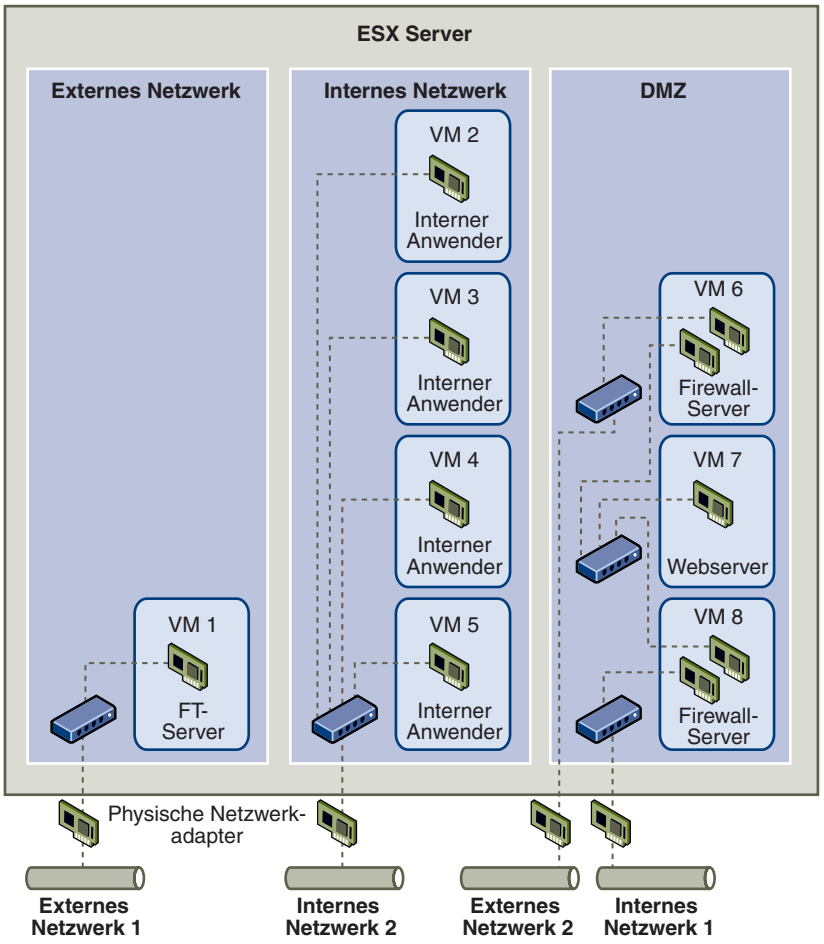


Abbildung 9-5. Externe Netzwerke, interne Netzwerke und DMZ auf einem ESX Server-Host

Hier wurde ein ESX Server-Host vom Systemadministrator in drei eigenständige VM-Zonen eingeteilt, von denen jede eine bestimmte Funktion erfüllt:

- **FTP-Server** – Die *virtuelle Maschine 1* wurde mit FTP-Software konfiguriert und fungiert als Sammelbecken für Daten von und an auswärtige Ressourcen, wie z. B. Formulardaten u. ä. von Anbietern.

  Diese virtuelle Maschine ist nur mit dem externen Netzwerk verbunden. Sie verfügt über ihren eigenen virtuellen Switch und ihren eigenen physischen Netzwerkadapter, die sie mit dem *externen Netzwerk 1* verbinden. Dieses Netzwerk ist auf Server beschränkt, die vom Unternehmen zum Empfang von Daten von ex-

ternen Quellen verwendet werden. Das Unternehmen verwendet beispielsweise das *Externe Netzwerk 1*, um FTP-Daten von Anbietern zu empfangen und den Anbietern FTP-Zugriff auf Daten, die auf extern verfügbaren Servern gespeichert sind, zu gewähren. Zusätzlich zur Verarbeitung der Daten für die *Virtuelle Maschine 1* verarbeitet das *Externe Netzwerk 1* auch Daten für FTP-Server auf anderen ESX Server-Hosts am Standort.

Da sich die *virtuelle Maschine 1* keinen virtuellen Switch oder physischen Netzwerkadapter mit anderen virtuellen Maschinen auf dem Host teilt, können die anderen virtuellen Maschinen auf dem Host keine Datenpakete in das Netzwerk der *virtuellen Maschine 1* übertragen oder daraus empfangen. Dadurch werden Abhörangriffe verhindert, da dem Opfer dafür Netzwerkdaten gesendet werden müssen. Außerdem kann der Angreifer dadurch die natürliche Anfälligkeit von FTP nicht zum Zugriff auf andere virtuelle Maschinen auf dem Host nutzen.

- Die **internen virtuellen Maschinen** – die *virtuellen Maschinen 2 – 5* sind der internen Verwendung vorbehalten. Diese virtuellen Maschinen verarbeiten und speichern empfindliche firmeninterne Daten wie medizinische Unterlagen, Gerichtsverfahren und Betrugsermittlungen. Daher müssen Systemadministratoren für diese virtuellen Maschinen den höchsten Schutz gewährleisten.

  Diese virtuellen Maschinen sind über ihren eigenen virtuellen Switch und physischen Netzwerkadapter an das *interne Netzwerk 2* angeschlossen. Das *interne Netzwerk 2* ist der internen Nutzung durch Mitarbeiter wie Reklamationssachbearbeiter, firmeneigene Anwälte und andere Sachbearbeiter vorbehalten.

  Die *virtuellen Maschinen 2 – 5* können über den virtuellen Switch untereinander und über den physischen Netzwerkadapter mit internen Maschinen an anderen Stellen des *internen Netzwerkes 2* kommunizieren. Sie können nicht mit Computern oder virtuellen Maschinen kommunizieren, die Zugang zu den externen Netzwerken haben. Wie beim FTP-Server können diese virtuellen Maschinen keine Datenpakete an Netzwerke anderer virtueller Maschinen senden oder sie von diesen empfangen. Ebenso können die anderen virtuellen Maschinen keine Datenpakete an die *virtuellen Maschinen 2 – 5* schicken oder von diesen empfangen.

- **DMZ** – Die *virtuellen Maschinen 6 – 8* wurden als DMZ konfiguriert, die von der Marketingabteilung dazu verwendet wird, die externe Website des Unternehmens bereitzustellen.

  Diese Gruppe der virtuellen Maschinen ist dem *Externen Netzwerk 2* und dem *Internen Netzwerk 1* zugeordnet. Das Unternehmen nutzt das *Externe Netzwerk 2* zur Unterstützung der Web-Server, die von der Marketing- und der Finanzabteilung zur Bereitstellung der Unternehmenswebsite und anderer web-basierter Anwendungen für externe Nutzer verwendet werden. Das *interne Netzwerk 1* ist der Verbindungskanal, den die Marketingabteilung zur Veröffentlichung von Webseiten auf der Unternehmenswebsite, zur Bereitstellung von Downloads und Diensten wie Anwenderforen verwendet.

Da diese Netzwerke vom *externen Netzwerk 1* und vom *internen Netzwerk 2* getrennt sind und die virtuellen Maschinen keine gemeinsamen Kontaktpunkte (Switches oder Adapter) aufweisen, besteht kein Angriffsrisiko für den FTP-Server oder die Gruppe interner virtueller Maschinen (weder als Ausgangspunkt noch als Ziel).

Ein Beispiel für die Konfiguration einer DMZ unter Verwendung von virtuellen Maschinen finden Sie unter „Beispiel: Erstellung einer Netzwerk-DMZ auf einem ESX Server-Host“ auf Seite 173.

Wenn die Isolierung der virtuellen Maschinen genau beachtet wird, die virtuellen Switches richtig konfiguriert werden und die Netzwerktrennung eingehalten wird, können alle drei Zonen virtueller Maschinen auf dem gleichen ESX Server-Host untergebracht werden, ohne dass Datenverluste oder Ressourcenangriffe befürchtet werden müssen.

Das Unternehmen erzwingt die Isolierung der VM-Gruppen durch die Verwendung mehrerer interner und externer Netzwerke und die Sicherstellung, dass die virtuellen Switches und physischen Netzwerkadapter jeder Gruppe von denen anderer Gruppen vollständig getrennt sind.

Da keiner der virtuellen Switches sich über mehrere Zonen erstreckt, wird das Risiko des Durchsickerns von Daten von einer Zone in eine andere ausgeschaltet. Ein virtueller Switch kann aufbaubedingt keine Datenpakete direkt an einen anderen virtuellen Switch weitergeben. Datenpakete können nur unter folgenden Umständen von einem virtuellen Switch zu einem anderen gelangen:

- Wenn die virtuellen Switches an das gleiche physische LAN angeschlossen sind.
- Wenn die virtuellen Switches an eine gemeinsame virtuelle Maschine angeschlossen sind, die dann dazu verwendet werden kann, Datenpakete zu übertragen.

In der Beispielkonfiguration wird keine dieser Bedingungen erfüllt. Wenn überprüft werden soll, dass es keinen gemeinsamen virtuellen Switch-Pfad gibt, kann dies über die Überprüfung möglicher gemeinsamer Kontaktpunkte im Netzwerkswitchplan im VI Client oder über VI-Web Access geschehen. Weitere Informationen zur Übersicht über die virtuellen Switches finden Sie unter „Virtuelle Switches“ auf Seite 23.

Zum Schutz der Hardware-Ressourcen der virtuellen Maschinen kann der Systemadministrator eine Reservierung und Begrenzung der Ressourcen für jede virtuelle Maschine vornehmen, um das Risiko für DOS- und DDOS-Angriffe einzuschränken. Der Systemadministrator kann den ESX Server-Host und die virtuellen Maschinen außerdem durch die Installation von Software-Firewalls an Front- und Backend der DMZ, durch Positionierung des ESX Server-Hosts hinter einer physischen Firewall und durch Anschluss der Servicekonsole und der an das Netzwerk angeschlossenen Speicherressourcen an jeweils einen eigenen virtuellen Switch schützen.

Sonstige Nachschlagewerke und Informationen zur Sicherheit

In folgenden Nachschlagewerken finden Sie zusätzliche Informationen zu Sicherheitsthemen.

Tabelle 9-1. Sicherheitsnachschlagewerke von VMware im Internet

Thema	Nachschlagewerk
Sicherheitsverfahren von VMware, aktuelle Sicherheitswarnungen, Sicherheitsdownloads und themenspezifische Abhandlungen zu Sicherheitslücken	**http://www.vmware.com/vmtn/technology/security**
Policy zur Sicherheitsantwort	**http://www.vmware.com/support/policies/security_response.html** VMware hat es sich zur Aufgabe gemacht, Sie bei der Absicherung Ihrer virtuellen Umgebung zu unterstützen. Damit Sie sicher sein können, dass alle Sicherheitslücken so schnell wie möglich eliminiert werden, haben wir die VMware Policy zur Sicherheitsantwort verfasst, um unseren Einsatz für dieses Ziel zu dokumentieren.
Zertifizierung von VMware Produkten	**http://www.vmware.com/security/** Wenn Sie den Zertifizierungsstatus bestimmter VMware Produkte suchen, führen Sie auf dieser Site eine Suche nach dem Begriff „VMware“ durch.
Unterstützung von Drittanbieter-Software	**http://www.vmware.com/support/policies** VMware unterstützt viele Speichersysteme und Software-Agenten wie Backup-Agenten, System-Management-Agenten usw. Ein Verzeichnis der von ESX Server unterstützten Agenten, Werkzeuge und anderer Software finden Sie durch die Suche nach ESX Server-Kompatibilitätshandbüchern unter **http://www.vmware.com/vmtn/resources**. Die Branche bietet mehr Produkte und Konfigurationen an, als VMware testen kann. Wenn VMware ein Produkt oder eine Konfiguration nicht in einem Kompatibilitätshandbuch nennt, wird die technische Unterstützung versuchen, Ihnen bei Problemen zu helfen, kann jedoch nicht garantieren, dass das Produkt oder die Konfiguration verwendet werden kann. Testen Sie die Sicherheitsrisiken für nicht unterstützte Produkte oder Konfigurationen immer sorgfältig.

Absicherung der ESX Server-Konfiguration 10

In diesem Kapitel werden die Maßnahmen beschrieben, mit denen Sie die Umgebung für Ihre ESX Server-Hosts, virtuellen Maschinen und iSCSI-SANs absichern können. Diese Abhandlung konzentriert sich auf den sicherheitsbezogenen Netzwerkkonfigurations-Aufbau und auf die Maßnahmen, mit denen Sie die Komponenten in Ihrer Konfiguration vor einem Angriff schützen können.

In diesem Kapitel werden folgende Themen behandelt:

- „Absicherung des Netzwerkes mit Firewalls“ auf Seite 181
- „Absicherung virtueller Maschinen durch VLANs“ auf Seite 194
- „Absicherung von iSCSI-Speicher“ auf Seite 204

Absicherung des Netzwerkes mit Firewalls

Sicherheitsadministratoren verwenden Firewalls, um das Netzwerk oder ausgewählte Komponenten innerhalb des Netzwerkes vor unerlaubten Zugriffen zu schützen. Firewalls kontrollieren den Zugriff auf die Geräte in ihrem Umfeld, indem sie alle Kommunikationspfade außer denen, die der Administrator explizit oder implizit als zulässig definiert, abriegeln. Dadurch wird die unerlaubte Verwendung der Geräte verhindert. Diese Pfade, die der Administrator in der Firewall öffnet, werden Ports genannt und lassen Datenverkehr zwischen Geräten auf den beiden Seiten der Firewall passieren.

In der VM-Umgebung können Firewalls in folgenden Varianten auftreten:

- Physische Maschinen wie z. B. VirtualCenter-Management-Server-Hosts und ESX Server Hosts.
- Zwischen zwei virtuellen Maschinen –zum Beispiel zwischen einer virtuellen Maschine, die als externer Web-Server dient, und einer virtuellen Maschine, die an das interne Unternehmensnetzwerk angeschlossen ist.

- Zwischen einem physischen Computer und einer virtuellen Maschine, wenn Sie eine Firewall zwischen einen physischen Netzwerkadapter und eine virtuelle Maschine schalten.

Die Nutzung von Firewalls in einer ESX Server-Konfiguration hängt davon ab, wie Sie das Netzwerk nutzen möchten und wie sicher die einzelnen Komponenten sein müssen. Wenn Sie zum Beispiel ein virtuelles Netzwerk erstellen, in dem jede virtuelle Maschine eine andere Benchmark-Testsuite für die gleiche Abteilung ausführt, ist das Risiko ungewollten Zugriffs von einer virtuellen Maschine auf eine andere minimal. So muss die Konfiguration vermutlich keine Firewalls zwischen den virtuellen Maschinen enthalten. Um eine Störung der Testläufe durch einen externen Host jedoch zu verhindern, kann die Konfiguration so eingerichtet werden, dass sich eine Firewall am Eingang zum virtuellen Netzwerk befindet, um alle virtuellen Maschinen zu schützen.

Dieser Abschnitt demonstriert die Aufstellung von Firewalls für Konfigurationen mit und ohne VirtualCenter. Hier finden Sie auch Informationen zu den Firewall-Ports, die für ESX Server-Systeme notwendig sind. In diesem Abschnitt werden folgende Themen behandelt:

- „Firewalls in Konfigurationen mit einem VirtualCenter Server“ auf Seite 182
- „Firewalls in Konfigurationen ohne VirtualCenter Server“ auf Seite 185
- „TCP- und UDP-Ports für den Management-Zugriff“ auf Seite 187
- „Verbindung zu einem VirtualCenter Server über eine Firewall“ auf Seite 189
- „Verbindung zur Konsole der virtuellen Maschine über eine Firewall“ auf Seite 189
- „Anbindung von ESX Server-Hosts über Firewalls“ auf Seite 191
- „Freigeben von Firewall-Ports für unterstützte Dienste und Management-Agenten“ auf Seite 192

Informationen zur Firewall der Servicekonsole finden Sie unter „Konfiguration der Servicekonsolen-Firewall“ auf Seite 240. Informationen zu Konfiguration und Port-Einstellungen während der Installation finden Sie im *Installations- und Upgrade-Handbuch*.

Firewalls in Konfigurationen mit einem VirtualCenter Server

Wenn Sie einen VirtualCenter Server verwenden, können Sie Firewalls an allen in der Abbildung Abbildung 10-1 gezeigten Punkten installieren.

HINWEIS Abhängig vom konkreten Aufbau sind ggf. nicht alle in der Abbildung dargestellten Firewalls notwendig, oder es sind zusätzliche, nicht dargestellte Firewalls nötig.

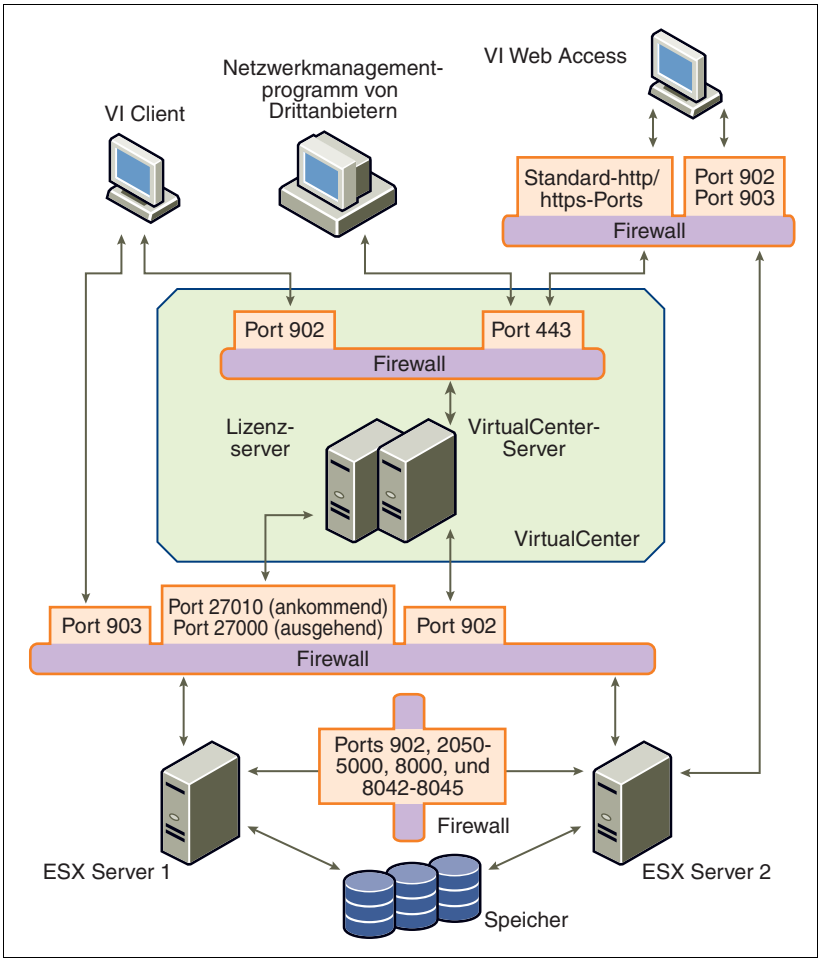


Abbildung 10-1. Firewallkonfiguration für ESX Server-Netzwerke, die über einen VirtualCenter Server verwaltet werden

Netzwerke, die über einen VirtualCenter Server konfiguriert werden, können Daten über verschiedene Typen von Clients erhalten: den VI Client, VI-Web Access und Netzwerk-Management-Clients von Drittanbietern, die SDK als Schnittstelle mit dem Host verwenden. Während des normalen Betriebs wartet VirtualCenter auf bestimmten Ports auf Daten von verwalteten Hosts und Clients. VirtualCenter geht auch davon aus, das die verwalteten Hosts auf bestimmten Ports auf Daten von VirtualCenter warten. Wenn sich zwischen diesen Elementen eine Firewall befindet, muss sichergestellt werden, dass in der Firewall Ports für den Datenverkehr freigegeben wurden.

Wenn Sie über einen VirtualCenter Server auf ESX Server-Hosts zugreifen, wird der VirtualCenter Server normalerweise durch eine Firewall geschützt. Diese Firewall bietet einen Grundschutz für das Netzwerk. Ob sich die Firewall zwischen den Clients und dem VirtualCenter Server befindet oder sowohl der VirtualCenter Server als auch die Clients hinter einer gemeinsamen Firewall liegen, hängt vom Netzwerkaufbau ab. Wichtig ist es sicherzustellen, dass eine Firewall an den Punkten installiert wird, die Sie als Eingangspunkte in das ganze System betrachten.

Firewalls können auch an vielen anderen Zugriffspunkten im Netzwerk installiert werden. Dies hängt davon ab, wie das Netzwerk genutzt werden soll und wie sicher die verschiedenen Geräte sein müssen. Bestimmen Sie die Installationspunkte für Ihre Firewalls anhand der Sicherheitsrisiken, die eine Analyse der Netzwerkkonfiguration ergeben hat. Die folgende Liste führt verschiedene Installationspunkte für Firewalls auf, die in ESX Server-Systemen häufig auftreten. Viele der Installationspunkte für Firewalls in der Liste und auf der Abbildung sind optional.

- Zwischen dem Webbrowser und den HTTP- und HTTPS-Proxy-Servern für VI-Web Access.
- Zwischen dem VI Client, VI-Web Access oder einem Netzwerk-Management-Client von Drittanbietern und dem VirtualCenter Server.
- Wenn die Anwender über den VI Client auf virtuelle Maschinen zugreifen: zwischen dem VI Client und dem ESX Server-Host. Diese Verbindung ist eine andere Verbindung als die zwischen dem VI Client und dem VirtualCenter Server und benötigt daher einen anderen Port.
- Wenn die Anwender über einen Webbrowser auf virtuelle Maschinen zugreifen: zwischen dem Webbrowser und dem ESX Server-Host. Diese Verbindung ist eine andere Verbindung als die zwischen dem VI-Web Access Client und dem VirtualCenter-Server und benötigt daher andere Ports.
- Zwischen dem Lizenz-Server und dem VirtualCenter Server oder dem ESX Server-Host. Normalerweise wird der Lizenz-Server in Konfigurationen mit einem VirtualCenter Server auf dem gleichen Computer ausgeführt wie der VirtualCenter-Server. In diesem Fall ist der Lizenz-Server über eine Firewall an das ESX Server-Netzwerk angebunden - parallel zum VirtualCenter Server, nur über andere Ports.

  In manchen Konfigurationen wird ggf. ein externer Lizenz-Server verwendet – zum Beispiel wenn das Unternehmen alle Lizenzen über ein einziges, für diesen Zweck dediziertes Gerät steuern möchte. In diesem Fall sollte der Lizenz-Server über eine zwischengeschaltete Firewall an den VirtualCenter Server angebunden werden.

  In jedem Fall sind die Ports, die für den Lizenzdatenverkehr verwendet werden, unabhängig von der Anbindung des Lizenz-Servers gleich. Weitere Informationen zur Lizenzierung finden Sie im *Installations- und und Upgrade-Handbuch*.
- Zwischen dem VirtualCenter Server und den ESX Server-Hosts.

- Zwischen den ESX Server-Hosts im Netzwerk. Zwar ist der Datenverkehr zwischen den ESX Server-Hosts normalerweise vertrauenswürdig, aber Sie können bei befürchteten Sicherheitsrisiken zwischen den einzelnen Computern dennoch Firewalls zwischen den ESX Server-Hosts installieren.

  Wenn Sie Firewalls zwischen ESX Server-Hosts verwenden und virtuelle Maschinen auf einen anderen Server verschieben, Cloning durchführen oder VMotion verwenden möchten, müssen auch Ports in allen Firewalls zwischen Quellhost und Zielhost geöffnet werden, damit Quelle und Ziel miteinander kommunizieren können.

- Zwischen ESX Server-Hosts und Peripheriegeräten wie z. B. NFS-Speicher. Diese Ports sind nicht VMware-spezifisch und werden anhand der Spezifikationen für das jeweilige Netzwerk konfiguriert.

Informationen zu den Ports, die für diese Kommunikationspfade geöffnet werden müssen, finden Sie unter „TCP- und UDP-Ports für den Management-Zugriff“ auf Seite 187.

Firewalls in Konfigurationen ohne VirtualCenter Server

Wenn die Clients direkt, nicht über den VirtualCenter Server, an das ESX Server-Netzwerk angebunden werden, gestaltet sich die Firewall-Anordnung etwas einfacher. Firewalls können an jeder der in Abbildung 10-2 abgebildeten Positionen installiert werden.

HINWEIS Abhängig vom konkreten Aufbau sind ggf. nicht alle in der Abbildung dargestellten Firewalls notwendig, oder es sind zusätzliche, nicht dargestellte Firewalls nötig.

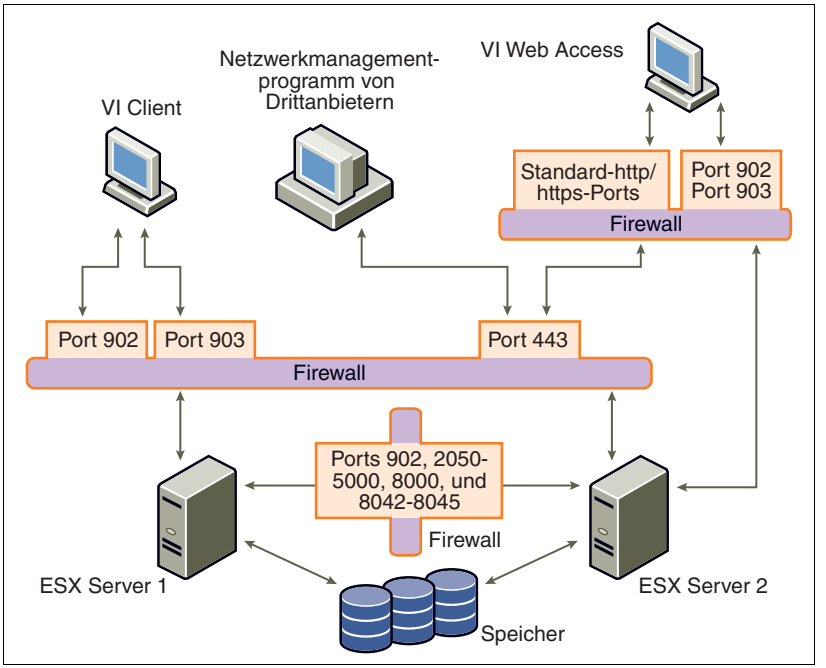


Abbildung 10-2. Firewallkonfiguration für ESX Server-Netzwerke, die direkt über einen Client verwaltet werden

Netzwerke ohne VirtualCenter Server erhalten ihre Daten über die gleichen Typen von Clients wie Netzwerke mit einem VirtualCenter Server: VI Client, VI-Web Access-Clients und Netzwerk-Management-Clients von Drittanbietern. Größtenteils sind die Anforderungen der Firewall die gleichen, aber es gibt einige markante Unterschiede:

- Wie bei Konfigurationen mit einem VirtualCenter Server sollten Sie sicherstellen, dass die ESX Server-Layer oder – je nach Aufbau – die Clients und die ESX Server-Layer geschützt sind. Diese Firewall bietet einen Grundschutz für das Netzwerk. Die verwendeten Firewall-Ports sind die gleichen wie bei der Verwendung eines VirtualCenter Servers.
- Die Lizenzierung gehört in dieser Konfiguration zu dem ESX Server-Paket, dass Sie auf allen ESX Server-Hosts installieren. Da die Lizenzierung über den Server abgewickelt wird, ist kein getrennter Lizenz-Server notwendig. Dadurch entfällt die Firewall zwischen dem Lizenz-Server und dem ESX Server-Netzwerk.

HINWEIS Unter bestimmten Umständen möchten Sie die Lizenzen zentral verwalten. Dazu können Sie einen getrennten Lizenz-Server verwenden oder den Lizenz-Server auf einem der ESX Server-Hosts im Netzwerk unterbringen. In beiden Fällen binden Sie den Lizenz-Server wie beim Vorhandensein eines Virtual-Center-Servers über eine Firewall an das ESX Server-Netzwerk an. Dazu werden die Ports verwendet, die normalerweise für die Lizenzierung von virtuellen Maschinen reserviert sind. Bei Konfigurationen, die einen anderen als den automatisch auf dem ESX Server-Host installierten Lizenz-Server verwenden, ist eine zusätzliche Einrichtung notwendig. Weitere Informationen zur Lizenzierung finden Sie im *Installations- und Upgrade-Handbuch*.

TCP- und UDP-Ports für den Management-Zugriff

In diesem Abschnitt werden voreingestellte TCP- und UDP-Ports, die für den Management-Zugriff auf den VirtualCenter Server, die ESX Server-Hosts und andere Netzwerkkomponenten verwendet werden, aufgeführt. Wenn Netzwerkkomponenten, die außerhalb einer Firewall liegen, verwaltet werden müssen, muss ggf. die Firewall neu konfiguriert werden, damit auf die entsprechenden Ports zugegriffen werden kann.

HINWEIS Sofern nicht anders angegeben, sind die in der Tabelle aufgeführten Ports durch die Servicekonsolenschnittstelle angebunden.

Tabelle 10-1. TCP- und UDP-Ports

Port	Zweck	Art des Datenverkehrs
80	HTTP-Zugriff. Nicht abgesicherter Standard-TCP-Webport, der normalerweise in Verbindung mit Port 443 als Front-End zum Zugriff auf ESX Server-Netzwerke vom Internet aus verwendet wird. Port 80 leitet Datenverkehr auf eine HTTPS-Startseite (Port 443) um, von der Sie die Konsole der virtuellen Maschine aufrufen. Verwenden Sie Port 80 für Verbindungen zu VI-Web Access vom Internet.	Eingehendes TCP
443	HTTPS-Zugriff. Der Standard-SSL-Internetport. Verwenden Sie Port 443 für folgende Aufgaben: ■ Verbindung zu VI-Web Access vom Internet. ■ VI-Web Access und Verbindungen von Netzwerk-Management-Clients von Drittanbietern an den VirtualCenter Server. ■ Direkter VI-Web Access und Zugriff der Netzwerk-Management-Clients von Drittanbietern auf ESX Server-Hosts.	Eingehendes TCP

Tabelle 10-1. TCP- und UDP-Ports (Fortsetzung)

Port	Zweck	Art des Datenverkehrs
902	Datenverkehr zur Authentifizierung für die Konfiguration von ESX Server-Host und virtuellen Maschinen. Verwenden Sie Port 902 für folgende Aufgaben: ■ VI Client-Zugriff auf den VirtualCenter Server. ■ VirtualCenter Server-Zugriff auf die ESX Server-Hosts. ■ Direkter VI Client-Zugriff auf die ESX Server-Hosts. ■ ESX Server-Hostzugriff auf andere ESX Server-Hosts für Migration und Provisioning.	Eingehendes TCP, abgehendes UDP
903	Datenverkehr der Remote-Steuerung, der durch Zugriffe der Anwender auf virtuelle Maschinen auf einem bestimmten ESX Server-Host entsteht. Verwenden Sie Port 903 für folgende Aufgaben: ■ VI Client-Zugriff auf die Konsolen von virtuellen Maschinen. ■ VI-Web Access Client-Zugriff auf die Konsolen von virtuellen Maschinen.	Eingehendes TCP
2049	Datenübertragungen von den NFS-Speichergeräten. Dieser Port wird auf der VMkernel-Schnittstelle, nicht auf der Servicekonsolenschnittstelle verwendet.	Eingehendes und abgehendes TCP
2050–5000	Datenverkehr zwischen ESX Server-Hosts für VMware Hochverfügbarkeit (HA) und den EMC Autostart Manager.	Abgehendes TCP, eingehendes und abgehendes UDP
3260	Datenübertragungen von den iSCSI-Speichergeräten. Dieser Port wird auf der VMkernel-Schnittstelle und auf der Servicekonsolenschnittstelle verwendet.	Abgehende TCP
8000	Eingehende Anfragen von VMotion. Dieser Port wird auf der VMkernel-Schnittstelle, nicht auf der Servicekonsolenschnittstelle verwendet.	Eingehendes und abgehendes TCP
8042–8045	Datenverkehr zwischen ESX Server-Hosts für VMware Hochverfügbarkeit (HA) und den EMC Autostart Manager.	Abgehendes TCP, eingehendes und abgehendes UDP
27000	Lizenzübertragungen vom ESX Server an den Lizenz-Server.	Abgehende TCP
27010	Lizenzübertragungen vom Lizenz-Server.	Eingehendes TCP

HINWEIS ESX Server und VirtualCenter verwenden intern die Ports 8085, 8087 und 9080. Für den ESX Server sind die Ports 8085, 8087 und 9080 geschützt, da sie keine Remote-Verbindungen akzeptieren.

Zusätzlich zu den aufgeführten TCP- und UDP-Ports können Sie andere Ports je nach Ihren Bedürfnissen konfigurieren:

- Mit VirtualCenter können Sie Ports für installierte Management-Agenten und unterstützte Dienste wie SSH, NFS usw. freigeben. Informationen zur Konfiguration anderer Ports für diese Dienste finden Sie unter „Freigeben von Firewall-Ports für unterstützte Dienste und Management-Agenten“ auf Seite 192.
- Für andere Dienste und Agenten, die für Ihr Netzwerk notwendig sind, können Sie Ports in der Firewall der Servicekonsole über Befehlszeilenskripte ausführen. Weitere Informationen finden Sie unter „Konfiguration der Servicekonsolen-Firewall“ auf Seite 240.

Verbindung zu einem VirtualCenter Server über eine Firewall

Wie in Tabelle 10-1 dargestellt, dass die Ports, die der VirtualCenter Server verwendet, während er auf Datenverkehr von seinen Clients wartet, die Ports 902 (VI Client) und 443 (andere Clients) sind. Wenn zwischen dem VirtualCenter Server und seinen Clients eine Firewall besteht, müssen Sie eine Verbindung konfigurieren, über die der VirtualCenter-Server Daten von seinen Clients empfangen kann.

Geben Sie in der Firewall Port 902 frei, damit der VirtualCenter Server Daten von einem VI Client empfangen kann. Geben Sie für Verbindungen zwischen dem VirtualCenter-Server und VI-Web Access-Clients oder Clients von Drittanbietern über das SDK Port 443 frei. Zusätzliche Informationen zur Konfiguration von Ports in einer Firewall erhalten Sie vom Firewall-Systemadministrator.

Wenn Sie den VI Client verwenden und nicht Port 902 als Port für den Datenverkehr zwischen VI Client und VirtualCenter Server verwenden möchten, können Sie den Port über die VirtualCenter-Einstellungen auf dem VI Client ändern. Informationen zur Änderung dieser Einstellungen finden Sie im *Benutzerhandbuch für die virtuelle Infrastruktur*.

Verbindung zur Konsole der virtuellen Maschine über eine Firewall

Sowohl bei der Anbindung des Clients an die ESX Server-Hosts über einen VirtualCenter-Server als auch bei der Verwendung einer direkten Verbindung an den ESX Server-Host sind bestimmte Hosts für die Kommunikation zwischen Administrator bzw. Anwender und den Konsolen der virtuellen Maschinen notwendig. Diese Ports unterstützen verschiedene Client-Funktionen, verbinden verschiedene Schichten innerhalb von ESX Server und verwenden verschiedene Authentifizierungsprotokolle. Dabei handelt es sich um:

- **Port 902** – VirtualCenter Server verwendet diesen Port, um Daten an die von VirtualCenter verwalteten Hosts zu senden. Auch der VI Client verwendet diesen Port, wenn er direkt mit dem ESX Server-Host verbunden ist, um Management-Funktionen für den Server und seine virtuellen Maschinen durchzuführen. Port 902 ist der Port, den der VirtualCenter Server und der VI Client für verfügbar halten, wenn sie Daten an den ESX Server-Host senden. Bei VMware kann für diese Verbindungen kein anderer Port konfiguriert werden.

Port 902 verbindet den VirtualCenter Server oder den Client über den VMware Authorization Daemon (`vmware-authd`), der in der Servicekonsole ausgeführt wird, mit dem ESX Server-Host. Der Authorization Daemon multiplext Daten von Port 902 zur Verarbeitung an den VMware Host Agent (`vmware-hostd`).

- **Port 443** – Der VI-Web Access-Client und SDK verwenden diesen Port, um Daten an die von VirtualCenter verwalteten Hosts zu senden. Der VI-Web Access-Client und SDK verwenden diesen Port auch, wenn sie direkt mit dem ESX Server-Host verbunden sind, um Management-Funktionen für den Server und seine virtuellen Maschinen durchzuführen. Port 443 ist der Port, den der VI-Web Access-Client und das SDK für verfügbar halten, wenn sie Daten an den ESX Server-Host senden. Bei VMware kann für diese Verbindungen kein anderer Port konfiguriert werden.

  Port 443 verbindet den VI-Web Access-Client oder Netzwerk-Management-Clients von Drittanbietern über den Tomcat Web-Dienst bzw. das SDK mit dem ESX Server-Host. Diese Prozesse multiplexen Daten von Port 443 zur Verarbeitung an `vmware-hostd`.

- **Port 903** – Der VI Client und VI-Web Access verwenden diesen Port für Verbindungen der Maus-/Tastatur-/Bildschirmaktivitäten des Gast-Betriebssystems auf virtuellen Maschinen. Die Anwender interagieren über diesen Port mit dem Gast-Betriebssystem und den Anwendungen der virtuellen Maschine. Port 903 ist der Port, den der VI Client und VI-Web Access für verfügbar halten, wenn sie mit virtuellen Maschinen kommunizieren. Bei VMware kann für diese Funktion kein anderer Port konfiguriert werden.

  Port 903 verbindet den VI Client mit einer bestimmten virtuellen Maschine, die auf dem ESX Server-Host konfiguriert wurde.

Abbildung 10-3 zeigt die Beziehungen zwischen VI Client-Funktionen, Ports und ESX Server-Prozessen. Der VI-Web Access-Client verwendet die gleiche Grundstruktur für seine Kommunikation mit dem ESX Server-Host.

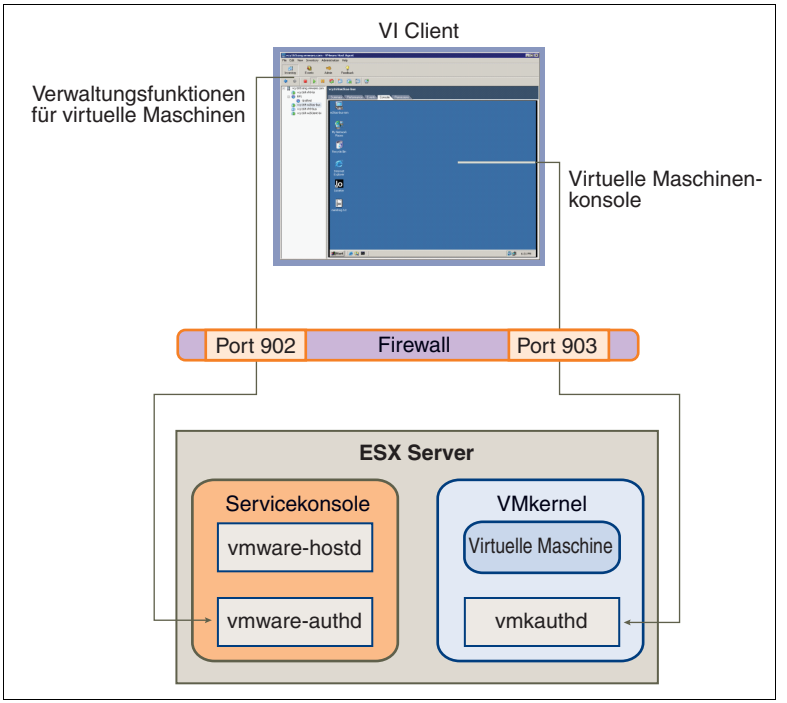


Abbildung 10-3. Port-Verwendung für VI Client-Datenverkehr mit ESX Server

Wenn Sie zwischen dem VirtualCenter Server und dem von VirtualCenter verwalteten Hosts eine Firewall installiert haben, müssen Sie Port 902 und 903 in der Firewall öffnen, um folgenden Datenverkehr zu ermöglichen:

- Vom VirtualCenter Server auf die ESX Server-Hosts.
- Direkt vom VI Client und von VI-Web Access auf die ESX Server-Hosts.

Weitere Informationen zur Konfiguration der Ports erhalten Sie beim Firewall-Systemadministrator.

Anbindung von ESX Server-Hosts über Firewalls

Wenn Sie eine Firewall zwischen zwei ESX Server-Hosts eingerichtet haben und Datenübertragungen zwischen den Hosts ermöglichen oder mit VirtualCenter Quelle-/Ziel-Aktivitäten wie Datenverkehr im Rahmen von VMware Hochverfügbarkeit (HA), Migrationen, Cloning oder VMotion durchführen möchten, müssen Sie eine Verbindung konfigurieren, über die die verwalteten Hosts Daten empfangen können. Dafür müssen Sie folgende Ports freigeben:

- 902 (Server-Server-Migration und Provisioning-Datenverkehr)
- 2050–5000 (für HA-Datenverkehr)

- 8000 (für VMotion)
- 8042–8045 (für HA-Datenverkehr)

Weitere Informationen zur Konfiguration der Ports erhalten Sie beim Firewall-Systemadministrator. Genauere Informationen zu Richtung und Protokollen für diese Ports finden Sie unter „TCP- und UDP-Ports für den Management-Zugriff“ auf Seite 187.

Freigeben von Firewall-Ports für unterstützte Dienste und Management-Agenten

Mit dem VI Client können Sie die Firewall der Servicekonsole so konfigurieren, dass die allgemein unterstützten Dienste und installierten Management-Agenten akzeptiert werden. Wenn Sie das Sicherheitsprofil des ESX Server-Hosts in VirtualCenter konfigurieren, werden durch das Hinzufügen oder Entfernen dieser Dienste oder Agenten automatisch festgelegte Ports freigegeben oder geschlossen, damit die Kommunikation mit dem Dienst oder dem Agenten möglich ist. Sie können folgende Dienste und Agenten hinzufügen oder entfernen:

- NIS-Client
- NFS-Client (unsicherer Dienst)
- SMB-Client (unsicherer Dienst)
- FTP-Client (unsicherer Dienst)
- SSH-Client
- Telnet-Client (unsicherer Dienst)
- NTP-Client
- iSCSI-Software-Client
- SSH-Server
- Telnet-Server (unsicherer Dienst)
- FTP-Server (unsicherer Dienst)
- NFS-Server (unsicherer Dienst)
- CIM-HTTP-Server (unsicherer Dienst)
- CIM-HTTPS-Server
- SNMP-Server
- Andere unterstützte Management-Agenten, die Sie installieren

HINWEIS Die aufgeführten Dienste und Agenten können sich ändern, d. h. der VI Client kann ggf. auch nicht aufgeführte Dienste und Agenten unterstützen. Außerdem werden nicht alle aufgeführten Dienste standardmäßig installiert. Zur Konfiguration und Aktivierung dieser Dienste sind gegebenenfalls weitere Schritte notwendig.

Wenn Sie ein Gerät, einen Dienst oder einen Agenten installieren, der nicht in der Liste aufgeführt wurde, müssen Sie über die Befehlszeile Ports in der Firewall der Servicekonsole freigeben. Weitere Informationen finden Sie unter „Konfiguration der Servicekonsolen-Firewall“ auf Seite 240.

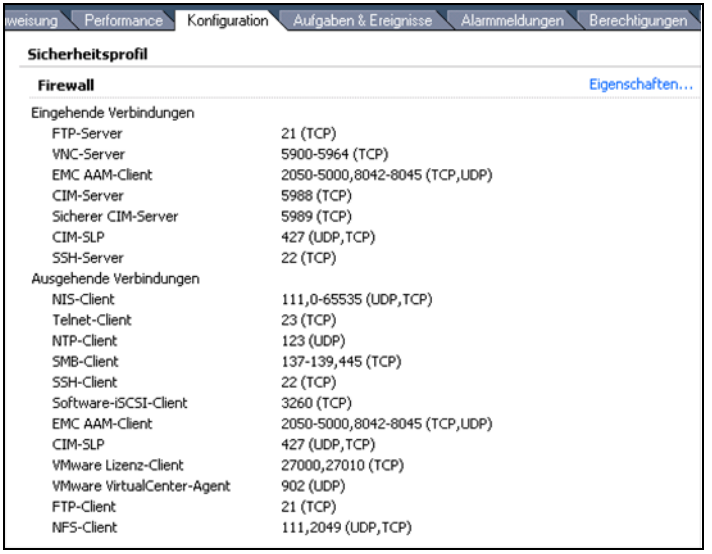
So ermöglichen Sie einem Dienst oder einem Management-Agenten den Zugriff auf ESX Server

1 Melden Sie sich am VI Client an und wählen Sie den Server aus dem Inventar aus.

Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

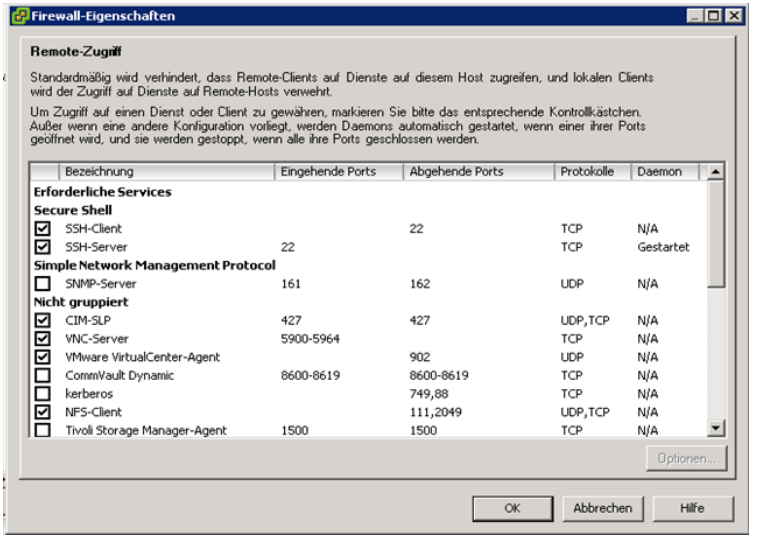
2 Klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Sicherheitsprofil**.

Der VI Client zeigt ein Verzeichnis der gegenwärtig aktiven eingehenden und ausgehenden Verbindungen mit den entsprechenden Firewall-Ports an.



3 Klicken Sie auf **Firewall** > **Eigenschaften**. Das Dialogfeld **Firewall Properties** (Firewall-Eigenschaften) wird geöffnet.

In diesem Dialogfeld werden alle Dienste und Management-Agenten, die Sie für den Host konfigurieren können, aufgelistet.


Firewall-Eigenschaften
Remote-Zugriff
Standardmäßig wird verhindert, dass Remote-Clients auf Dienste auf diesem Host zugreifen, und lokalen Clients wird der Zugriff auf Dienste auf Remote-Hosts verwehrt.
Um Zugriff auf einen Dienst oder Client zu gewähren, markieren Sie bitte das entsprechende Kontrollkästchen. Außer wenn eine andere Konfiguration vorliegt, werden Daemons automatisch gestartet, wenn einer ihrer Ports geöffnet wird, und sie werden gestoppt, wenn alle ihre Ports geschlossen werden.
Bezeichnung
Eingehende Ports
Abgehende Ports
Protokolle
Daemon
Erforderliche Services
Secure Shell
SSH-Client 22 TCP N/A
SSH-Server 22 TCP Gestartet
Simple Network Management Protocol
SNMP-Server 161 162 UDP N/A
Nicht gruppiert
CIM-SLP 427 427 UDP,TCP N/A
VNC-Server 5900-5964 TCP N/A
VMware VirtualCenter-Agent 902 UDP N/A
CommVault Dynamic 8600-8619 8600-8619 TCP N/A
kerberos 749,88 TCP N/A
NFS-Client 111,2049 UDP,TCP N/A
Tivoli Storage Manager-Agent 1500 1500 TCP N/A
Optionen...
OK
Abbrechen
Hilfe

4 Aktivieren Sie die Kontrollkästchen für die Dienste und Agenten, die Sie aktivieren möchten.

   Die Spalten **Eingehende Ports** und **Ausgehende Ports** zeigen die Ports an, die der VI Client für einen Dienst freigibt; die Spalte **Protokoll** gibt das Protokoll an, das der Dienst verwendet, und die Spalte **Daemon** zeigt den Status des Daemons an, der dem Dienst zugewiesen wurde.

5 Klicken Sie auf **OK**.

Absicherung virtueller Maschinen durch VLANs

Das Netzwerk gehört zu den gefährdetsten Teilen des Systems. Ein virtuelles Netzwerk benötigt daher ebenso wie ein physisches Netzwerk Schutz. Wenn das Netzwerk virtueller Maschinen an ein physisches Netzwerk angeschlossen ist, kann es ebenso Sicherheitslücken aufweisen wie ein Netzwerk, das aus physischen Computern besteht. Selbst wenn das VM-Netzwerk nicht an ein physisches Netzwerk angeschlossen ist, kann ein Angriff auf virtuelle Maschinen innerhalb des Netzwerks von anderen virtuellen Maschinen des Netzwerkes aus erfolgen. Die Anforderungen an die Absicherung von virtuellen Maschinen sind oft die gleichen wie für physische Maschinen.

Virtuelle Maschinen sind voneinander isoliert: Eine virtuelle Maschine kann nicht im Speicher der anderen virtuellen Maschine schreiben oder lesen, auf deren Daten zugreifen, ihre Anwendungen verwenden usw. Im Netzwerk kann jedoch jede virtuelle Maschine oder eine Gruppe von virtuellen Maschinen Ziel eines unerlaubten Zugriffs von anderen virtuellen Maschinen sein und daher weiteren Schutzes durch externe Maßnahmen bedürfen. Dies können Sie durch folgende Maßnahmen erreichen:

- Firewallschutz für das virtuelle Netzwerk durch Installation und Konfiguration von Software-Firewalls auf einigen oder allen virtuellen Maschinen im Netzwerk.

HINWEIS Aus Effizienzgründen können Sie private Ethernet-Netzwerke virtueller Maschinen oder *Virtuelle Netzwerke* einrichten. Bei virtuellen Netzwerken installieren Sie eine Software-Firewall auf einer virtuellen Maschine am Eingang des virtuellen Netzwerks. Diese dient als Schutzpufferzone zwischen dem physischen Netzwerkadapter und den übrigen virtuellen Maschinen im virtuellen Netzwerk.

Die Installation einer Software-Firewall auf virtuellen Maschinen am Eingang eines virtuellen Netzwerkes ist eine bewährte Sicherheitsmaßnahme. Da jedoch Software-Firewalls die Leistung verlangsamen können, sollten Sie Sicherheitsbedürfnisse und Leistungsanforderungen abwägen, bevor Sie Software-Firewalls auf anderen virtuellen Maschinen im Netzwerk installieren. Weitere Informationen zu virtuellen Netzwerken finden Sie unter „Netzwerk-Konzepte“ auf Seite 22.

- Beibehalten verschiedener Zonen aus virtuellen Maschinen innerhalb eines Hosts auf verschiedenen Netzwerksegmenten. Wenn Sie virtuelle Maschinenzonen auf deren eigenen Netzwerksegmenten isolieren, minimieren Sie das Risiko eines Datenverlusts aus einer virtuellen Maschinenzone auf die Nächste. Die Segmentierung verhindert mehrere Gefahren. Zu diesen Gefahren gehört auch die Manipulation des Adressauflösungsprotokolls (ARP), wobei der Angreifer die ARP-Tabelle so manipuliert, dass die MAC- und IP-Adressen neu zugeordnet werden. wodurch der Zugriff auf den Netzwerkdatenverkehr vom und zum Host möglich ist. Angreifer verwenden diese ARP-Manipulierung für Dienstblockaden (DOS), zur Übernahme des Zielsystems und zur anderweitigen Beeinträchtigung des virtuellen Netzwerks.

  Eine sorgfältige Planung der Segmentierung senkt das Risiko von Paket- Übertragungen zwischen virtuellen Maschinenzonen und somit Spionageangriffe, die voraussetzen, dass dem Opfer Netzwerk-Datenverkehr zugestellt wird. So kann ein Angreifer auch keinen unsicheren Service in einer virtuellen Maschinenzone aktivieren, um auf andere virtuelle Maschinenzonen im Host zuzugreifen. Gegen verschiedene Sicherheitsrisiken. Sie können die Segmentierung mit einer der beiden Methoden herstellen, von denen jede andere Vorteile bietet.

  - Verwenden Sie getrennte physische Netzwerkadapter für Zonen virtueller Maschinen, damit die Zonen auch tatsächlich voneinander getrennt sind. Die Beibehaltung getrennter physischer Netzwerkadapter für die virtuellen Maschinenzonen stellt unter Umständen die sicherste Methode dar und gleichzeitig ist sie am wenigsten anfällig für Konfigurationsfehler nach dem Anlegen des ersten Segments.
  - Einrichtung von virtuellen LANs (VLANs) zur Absicherung des Netzwerkes. Da VLANs fast alle Sicherheitsvorteile bieten, die auch die Implementation physisch getrennter Netzwerke aufweist, ohne dass dafür der Hardware-Overhead eines physischen Netzwerkes notwendig ist, stellen sie eine rentable Lösung zur Verfügung, die die Kosten für die Bereitstellung und Wartung zusätzlicher Geräte, Kabel usw. einsparen kann.

VLANs sind eine Netzwerkarchitektur nach dem IEEE-Standard und verfügen über spezifische Kennzeichnungsmethoden, durch die Datenpakete nur an die Ports weitergeleitet werden, die zum VLAN gehören. Wenn das VLAN richtig konfiguriert ist, ist es ein zuverlässiges Mittel zum Schutz einer Gruppe virtueller Maschinen vor zufälligem und böswilligem Eindringen.

Mit VLANs können Sie ein physisches Netzwerk so in Segmente aufteilen, dass zwei Computer oder virtuelle Maschinen im Netzwerk nur dann Pakete untereinander austauschen können, wenn sie zum gleichen VLAN gehören. So gehören zum Beispiel Buchhaltungsunterlagen und -transaktionen zu den wichtigsten vertraulichen internen Informationen eines Unternehmens. Wenn in einem Unternehmen die virtuellen Maschinen der Verkaufs-, der Logistik- und der Buchhaltungsangestellten an das gleiche physische Netzwerk angeschlossen sind, können Sie die virtuellen Maschinen für die Buchhaltungsabteilung schützen, indem Sie VLANs wie in der Abbildung Abbildung 10-4 einrichten.

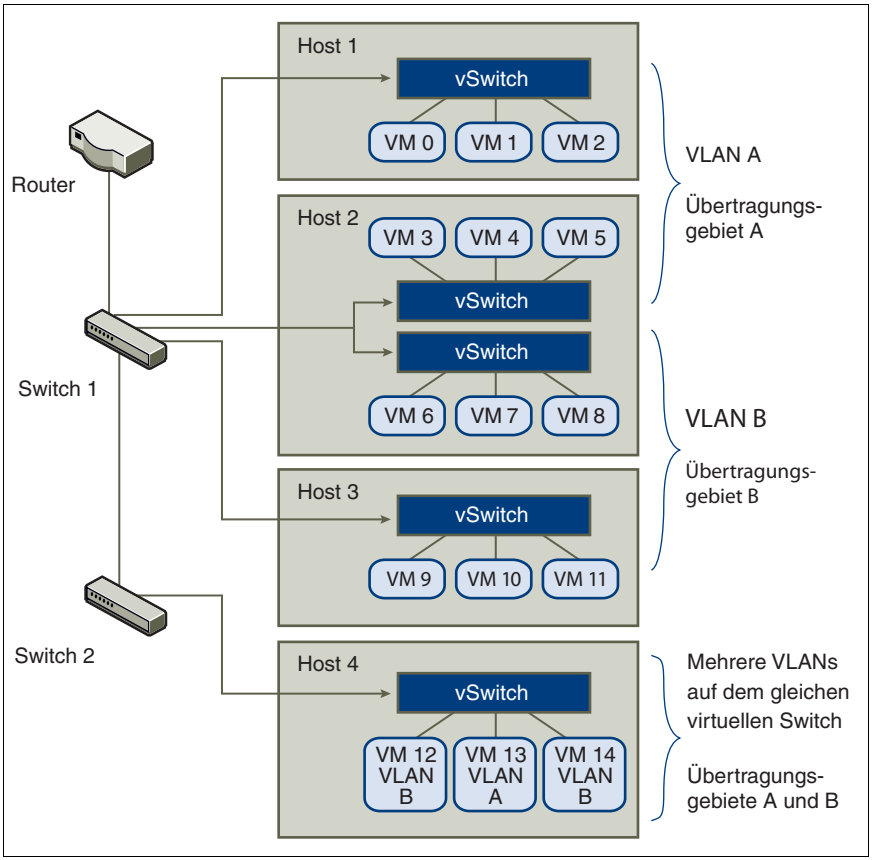


Abbildung 10-4. Beispiel-VLAN-Plan

In dieser Konfiguration verwenden alle Angestellten der Buchhaltungsabteilung virtuelle Maschinen im *VLAN A*, die Angestellten der Verkaufsabteilung verwenden die virtuellen Maschinen im *VLAN B*.

Der Router leitet die Datenpakete mit Buchhaltungsdaten an die Switches weiter. Diese Pakete sind so gekennzeichnet, dass sie nur an *VLAN A* weitergeleitet werden dürfen. Daher sind die Daten auf *Übertragungsgebiet A* beschränkt und können nur an das *Übertragungsgebiet B* weitergeleitet werden, wenn der Router entsprechend konfiguriert wurde.

In dieser VLAN-Konfiguration wird verhindert, dass Mitarbeiter der Verkaufsabteilung Datenpakete, die für die Buchhaltungsabteilung bestimmt sind, abfangen können. Die Buchhaltungsabteilung kann auch keine Datenpakete empfangen, die für die Verkaufsabteilung bestimmt sind. Beachten Sie, dass sich virtuelle Maschinen, die an einen gemeinsamen virtuellen Switch angebunden sind, dennoch in unterschiedlichen VLANs befinden können.

Im folgenden Abschnitt finden Sie Vorschläge zur Absicherung des Netzwerkes über virtuelle Switches und VLANs. In diesem Abschnitt werden folgende Themen behandelt:

- „Sicherheitsempfehlungen für VLANs“ auf Seite 197
- „Schutz durch virtuelle Switches in VLANs“ auf Seite 199
- „Absicherung der Ports virtueller Switches“ auf Seite 201

Sicherheitsempfehlungen für VLANs

ESX Server ist mit einer vollständigen VLAN-Implementierung nach IEEE 802.1q ausgestattet. Wie Sie die VLANs einrichten, um Teile eines Netzwerkes abzusichern, hängt von Faktoren wie dem installierten Gast-Betriebssystem, der Konfiguration der Netzwerkgeräte usw. ab. Zwar kann VMware keine spezifischen Empfehlungen aussprechen, wie die VLANs eingerichtet werden sollten, folgende Faktoren sollten jedoch berücksichtigt werden, wenn Sie VLANs als Teil der Sicherheitsmaßnahmen einsetzen:

- **Setzen Sie VLANs im Rahmen eines Sicherheitspakets ein** – mit VLANs kann effektiv gesteuert werden, wo und in welchem Umfang Daten im Netzwerk übertragen werden. Wenn ein Angreifer Zugang zum Netzwerk erlangt, wird der Angriff mit hoher Wahrscheinlichkeit nur auf das VLAN beschränkt, das als Zugangspunkt diente, wodurch das Risiko für das gesamte Netzwerk verringert wird.

  VLANs bieten nur dadurch Schutz, dass sie steuern, wie Daten weitergeleitet und verarbeitet werden, nachdem sie die Switches passiert haben und sich im Netzerk befinden. Sie können VLANs dazu nutzen, Layer 2 des Netzwerkmodells – die Sicherungsschicht – zu schützen. Die Einrichtung von VLANs schützt jedoch weder die Bitübertragungsschicht noch die anderen Schichten. Auch bei der Verwendung von VLANs sollten Sie zusätzlichen Schutz durch Absicherung der Hardware (Router, Hubs usw.) und Verschlüsselung der Datenübertragungen implementieren.

VLANs ersetzen die Software-Firewalls in den virtuellen Maschinen nicht. In den meisten Netzwerkkonfigurationen mit VLANs gibt es auch Software-Firewalls. Wenn Sie VLANs in Ihr virtuelles Netzwerk implementieren, müssen die Firewalls VLANs erkennen können.

- **Stellen Sie sicher, dass die VLANs ordnungsgemäß konfiguriert sind** – Eine Fehlkonfiguration der Ausstattung und Netzwerk-Hardware, Firmware oder der Software setzt ein VLAN möglichen VLAN-Hopping-Angriffen aus. VLAN-Hopping tritt dann auf, wenn ein Angreifer mit autorisiertem Zugriff auf ein VLAN Datenpakete erstellt, die die physischen Switches dazu bringen, die Pakete in ein anderes VLAN zu übertragen, für das der Angreifer keine Zugriffsberechtigung besitzt. Anfälligkeit für diese Art von Angriffen liegt meist dann vor, wenn ein Switch falsch für den nativen VLAN-Betrieb konfiguriert wurde, wodurch der Switch nicht gekennzeichnete Pakete empfangen und übertragen kann.

  Um ein VLAN-Hopping zu verhindern, aktualisieren Sie stets Ihre Ausstattung, indem Sie Updates der Hardware und Firmware sofort aufspielen. Achten Sie bei der Konfiguration Ihrer Anlagen auch stets auf die Einhaltung der Best Practices Ihres Händlers.

  Bitte bedenken Sie, dass die virtuellen Switches von VMware das Konzept nativer VLANs nicht unterstützen. Alle Daten, die über diese Switches übertragen werden, müssen ordnungsgemäß gekennzeichnet werden. Da es jedoch im Netzwerk auch andere Switches geben kann, die für den nativen VLAN-Betrieb konfiguriert wurden, können VLANs mit virtuellen Switches dennoch anfällig für VLAN-Hopping sein.

  Wenn Sie VLANs zur Netzwerksicherung verwenden möchten, empfiehlt VMware, die native VLAN-Funktion für alle Switches zu deaktiveren, sofern nicht ein zwingender Grund vorliegt, dass einige VLANs im nativen Modus betrieben werden müssen. Wenn Sie ein natives VLAN verwenden müssen, beachten Sie die Konfigurationsrichtlinien des Switch-Herstellers für diese Funktion.

- **Richten Sie ein eigenes VLAN bzw. einen eigenen virtuellen Switch für die Kommunikation zwischen den Management-Tools und der Servicekonsole ein** – Sowohl bei der Verwendung eines Management-Clients als auch der Befehlszeile werden alle Konfigurationsaufgaben für ESX Server wie z. B. Speicher, Steuerungsaspekte des Verhaltens virtueller Maschinen oder die Einrichtung von virtuellen Switches oder virtuellen Netzwerken über die Servicekonsole ausgeführt. Da die Servicekonsole die Steuerungszentrale von ESX Server ist, ist ihr Schutz vor Missbrauch besonders wichtig.

  Zwar verwenden die Managementclients von VMware ESX Server Authentifizierung und Verschlüsselung, um unerlaubten Zugriff auf die Servicekonsole zu verhindern, aber andere Dienste bieten ggf. nicht den gleichen Schutz. Wenn Angreifer Zugriff auf die Servicekonsole erlangen, können sie viele Attribute des ESX Server-Hosts neu konfigurieren. So können Sie zum Beispiel die gesamte Konfiguration der virtuellen Switches oder die Autorisierungsverfahren usw. ändern.

Die Netzwerkanbindung für die Servicekonsole wird über virtuelle Switches hergestellt. Um diese wichtigen ESX Server-Komponenten zu schützen, empfiehlt VMware die Isolierung der Servicekonsole durch eines der folgenden Verfahren:

- Richten Sie ein VLAN für die Kommunikation der Management-Tools mit der Servicekonsole ein.
- Konfigurieren Sie den Netzwerkzugang für die Management-Tool-Verbindungen mit der Servicekonsole über einen einzigen virtuellen Switch und einen oder mehrere Uplink-Ports.

Beide Methoden verhindern, dass jemand ohne Zugriff auf das Servicekonsolen-VLAN oder den virtuellen Switch, den eingehenden und ausgehenden Datenverkehr der Servicekonsole sehen kann. Außerdem können so Angreifer keine Pakete an die Servicekonsole senden. Alternativ können Sie stattdessen die Servicekonsole auf einem eigenen physischen Netzwerksegment konfigurieren. Die physische Segmentierung bietet eine gewisse zusätzliche Sicherheit, da diese vor einer späteren Fehlkonfiguration schützt.

Zusätzlich zur Einrichtung eines eigenen VLANs oder virtuellen Switches für die Kommunikation der Management-Tools mit der Servicekonsole sollten Sie ein eigenes VLAN oder einen eigenen virtuellen Switch für VMotion und für Netzwerkspeicher einrichten.

HINWEIS Wenn Ihre Konfiguration ein iSCSI-SAN umfasst, das direkt durch den Host und nicht durch den Hardware-Adapter konfiguriert wurde, sollten Sie einen eigenen virtuellen Switch anlegen, der eine gemeinsam genutzte Netzwerk-Konnektivität für die Servicekonsole und für iSCSI bietet. Diese zweite Netzwerkverbindung für die Servicekonsole besteht zusätzlich zur primären Servicekonsolen-Netzwerkverbindung, die Sie für die Kommunikation Ihrer Management-Tools verwenden. Die zweite Servicekonsolen-Netzwerkverbindung unterstützt nur die iSCSI-Aktivitäten und Sie sollten Sie nicht für Management-Aktivitäten oder die Management-Tool-Kommunikation verwenden.

Schutz durch virtuelle Switches in VLANs

Die virtuellen Switches von VMware schützen gegen bestimmte Gefahren von VLANs. Durch den Aufbau der virtuellen Switches schützen sie VLANs gegen viele Arten von Angriffen, die meist auf VLAN-Hopping basieren. Dieser Schutz garantiert jedoch nicht, dass Ihre virtuellen Maschinen gegen andere Arten von Angriffen immun sind. So schützen virtuelle Switches zum Beispiel nicht das physische Netzwerk vor diesen Angriffen, sondern nur das virtuelle Netzwerk.

Die folgende Liste vermittelt Ihnen die Grundlagen zu einigen Angriffsarten, gegen die virtuelle Switches und VLANs schützen können.

- **MAC-Flooding** – Diese Angriffe überschwemmen den Switch mit Datenpaketen, die MAC-Adressen enthalten, die als von verschiedenen Quellen stammend gekennzeichnet wurden. Viele Switches verwenden eine assoziative Speichertabelle (CAM-Tabelle), um die Quelladresse für jedes Datenpaket zu speichern. Wenn die Tabelle voll ist, schaltet der Switch ggf. in einen vollständig geöffneten Status um, in dem alle eingehenden Pakete auf allen Ports übertragen werden, sodass der Angreifer den gesamten Datenverkehr des Switches abhören kann. In diesem Fall kann es auch zu Paketlecks in andere VLANs kommen.

  Zwar speichern die virtuellen Switches von VMware eine MAC-Adressentabelle, aber sie erhalten die MAC-Adressen nicht von abhörbaren Datenverkehr und sind daher gegen diese Art von Angriffen immun.

- **Angriffe durch 802.1q- und ISL-Kennzeichnung** – Bei diesem Angriff werden die Datenblöcke durch den Switch an ein anderes VLAN weitergeleitet, indem der Switch durch einen Trick dazu gebracht wird, als Trunk zu fungieren und den Datenverkehr an andere VLANs weiterzuleiten.

  Die virtuellen Switches von VMware führen das dynamische Trunking, das für diese Art des Angriffes notwendig ist, nicht aus, und sind daher immun.

- **Doppelt eingekapselte Angriffe** – Bei dieser Art von Angriffen erstellt der Angreifer ein doppelt eingekapseltes Paket, in dem sich der VLAN-Bezeichner im inneren Tag vom VLAN-Bezeichner im äußeren Tag unterscheidet. Um Rückwärtskompatibilität zu gewährleisten, entfernen native VLANs standardmäßig das äußere Tag von übertragenen Paketen. Wenn ein nativer VLAN-Switch das äußere Tag entfernt, bleibt nur das innere Tag übrig, welches das Paket zu einem anderen VLAN weiterleitet, als im jetzt fehlenden äußeren Tag angegeben war.

  Die virtuellen Switches von VMware verwerfen alle doppelt eingekapselten Datenblöcke, die eine virtuelle Maschine auf einem für ein bestimmtes VLAN konfigurierten Port senden möchte. Daher sind sie immun gegen diese Art von Angriffen.

- **Multicast-Brute-Force-Angriffe** – Bei diesen Angriffen wird eine große Anzahl von Multicast-Datenblöcken fast zeitgleich an ein bekanntes VLAN gesendet, um den Switch zu überfordern, sodass er versehentlich einige Datenblöcke in andere VLANs überträgt.

  Die virtuellen Switches von VMware erlauben es Datenblöcken nicht, ihren richtigen Übertragungsbereich (VLAN) zu verlassen und sind daher gegen diese Art von Angriffen immun.

- **Spanning-Tree-Angriffe** – Diese Angriffe zielen auf das Spanning-Tree-Protokoll (STP), das zur Steuerung der Überbrückung verschiedener Teile des LANs verwendet wird. Der Angreifer sendet Pakete der Bridge Protocol Data Unit (BPDU) in dem Versuch, die Netzwerktopologie zu ändern und sich selbst als Root-Bridge einzusetzen. Als Root-Bridge kann der Angreifer dann die Inhalte übertragener Datenblöcke mitschneiden.

Die virtuellen Switches von VMware unterstützen STP nicht und sind daher gegen diese Art von Angriffen immun.

- **Zufallsdatenblock-Angriffe** – Bei diesen Angriffen wird eine große Anzahl von Paketen, bei denen die Quell- und Zieladressen gleich sind, die jedoch Felder unterschiedlicher Länge, Art und mit verschiedenem Inhalt enthalten, versendet. Ziel des Angriffes ist es zu erzwingen, dass Pakete versehentlich in ein anderes VLAN fehlgeleitet werden.

  Die virtuellen Switches von VMware sind gegen diese Art von Angriffen immun.

Da mit der Zeit immer neue Sicherheitsgefahren auftreten, kann diese Liste möglicher Angriffe nicht vollständig sein. Konsultieren Sie regelmäßig die VMware Sicherheits-Ressourcen im Internet (**http://www.vmware.com/vmtn/technology/security**), um mehr über Sicherheit, neue Sicherheitswarnungen und die Sicherheitstaktik von VMware zu erfahren.

Absicherung der Ports virtueller Switches

Wie bei physischen Netzwerkadaptern kann ein virtueller Netzwerkadapter Datenblöcke versenden, die von einer anderen virtuellen Maschine zu stammen scheinen oder eine andere virtuelle Maschine imitieren, damit er Datenblöcke aus dem Netzwerk empfangen kann, die für die jeweilige virtuelle Maschine bestimmt sind. Außerdem kann ein virtueller Netzwerkadapter, genauso wie ein physischer Netzwerkadapter, so konfiguriert werden, dass er Datenblöcke empfängt, die für andere virtuelle Maschinen bestimmt sind.

Wenn Sie einen virtuellen Switch für Ihr Netzwerk erstellen, fügen Sie Port-Gruppen hinzu, um für die an den Switch angeschlossenen virtuellen Maschinen, Speichersysteme usw. Policys zu konfigurieren. Virtuelle Switches werden über den VI Client erstellt.

Während des Hinzufügens eines Ports oder einer Port-Gruppe zu einem virtuellen Switch konfiguriert der VI Client ein Sicherheitsprofil für den Port. Mit diesem Sicherheitsprofil können Sie sicherstellen, dass ESX Server verhindert, dass die Gast-Betriebssysteme auf den virtuellen Maschinen andere VMs im Netzwerk imitieren können. Diese Sicherheitsfunktion wurde so implementiert, dass das Gast-Betriebssystem, das für die Imitation verantwortlich ist, nicht erkennt, dass diese verhindert wurde.

Das Sicherheitsprofil bestimmt, wie streng der Schutz gegen Imitierungs- oder Abfangangriffe auf virtuelle Maschinen sein soll. Damit Sie die Einstellungen des Sicherheitsprofils richtig anwenden können, benötigen Sie Grundkenntnisse darüber, wie virtuelle Netzwerkadapter Datenübertragungen steuern und wie Angriffe auf dieser Ebene vorgenommen werden.

Jedem virtuellen Netzwerkadapter wird bei seiner Erstellung eine eindeutige MAC-Adresse zugewiesen. Diese Adresse wird „Ursprünglich zugewiesene MAC-Adresse“ genannt. Obwohl die ursprüngliche MAC-Adresse von außerhalb des Gast-Betriebssystems neu konfiguriert werden kann, kann sie nicht vom Gastbetriebssystem selbst geändert werden. Außerdem verfügt jeder Adapter über eine geltende MAC-Adresse, die

eingehenden Netzwerkverkehr mit einer MAC-Adresse, die nicht der geltenden MAC-Adresse entspricht, ausfiltert. Das Gast-Betriebssystem ist für die Einstellung der geltenden MAC-Adresse verantwortlich. In der Regel stimmen die geltende MAC-Adresse und die ursprünglich zugewiesene MAC-Adresse überein.

Beim Versand von Datenpaketen schreibt das Betriebssystem die wirksame MAC-Adresse des eigenen Netzwerkadapters in das Feld „Quell-MAC-Adresse“ des Ethernet-Frames. Es schreibt auch die MAC-Adresse des Empfänger-Netzwerkadapters in das Feld „Ziel-MAC-Adresse“. Der empfangende Adapter akzeptiert Datenpakete nur dann, wenn die Ziel-MAC-Adresse im Paket mit seiner eigenen geltenden MAC-Adresse übereinstimmt.

Bei der Erstellung stimmen die geltende und die ursprünglich zugewiesene MAC- Adresse überein. Das Betriebssystem der virtuellen Maschine kann die geltenden MAC- Adresse jedoch jederzeit auf einen anderen Wert setzen. Wenn ein Betriebssystem die geltenden MAC-Adresse ändert, empfängt der Netzwerkadapter Netzwerk datenverkehr, der für die neue MAC-Adresse bestimmt ist. Das Betriebssystem kann jederzeit Frames mit einer imitierten Quell-MAC-Adresse senden. Daher kann ein Betriebssystem böswillige Angriffe auf die Geräte in einem Netzwerk durchführen, indem es einen Netzwerkadapter imitiert, der vom Empfängernetzwerk autorisiert wurde.

Mit den Sicherheitsprofilen für den virtuellen Switch auf den ESX Server-Hosts können Sie sich gegen diese Art von Angriffen schützen, indem Sie drei Optionen einstellen:

- **MAC-Adressänderungen** – In der Standardeinstellung ist diese Option auf **Akzeptieren** gesetzt, d. h. dass der ESX Server-Host Anfragen, die geltende MAC-Adresse in eine andere als die ursprünglich zugewiesene Adresse zu ändern, akzeptiert. Die Einstellungen der Option **MAC-Adressen-Änderung** beeinflusst den Datenverkehr, den eine virtuelle Maschine empfängt.

  Zum Schutz gegen MAC-Imitation können Sie diese Option auf **Reject** (Ablehnen) setzen. In diesem Fall lehnt der ESX Server-Host alle Anfragen, die geltende MAC-Adresse in eine andere als die ursprünglich zugewiesene Adresse zu ändern, ab. Stattdessen wird der Port, der von dem virtuellen Adapter zum Senden der Anfrage verwendet wird, deaktiviert. Als Folge erhält der virtuelle Adapter keine weiteren Datenpakete mehr, bis er die geltende MAC-Adresse ändert, sodass sie mit der ursprünglichen MAC-Adresse übereinstimmt. Das Gast-Betriebssystem erkennt nicht, dass die Änderung der MAC-Adresse nicht angenommen wurde.

HINWEIS In bestimmten Situationen ist es tatsächlich notwendig, dass mehrere Adapter in einem Netzwerk die gleiche MAC-Adresse haben – zum Beispiel, wenn Sie Microsoft-Netzwerklastausgleich (NLB) im Unicast-Modus verwenden. Bei der Verwendung von Microsoft NLB im Standard-Multicast-Modus haben die Adapter nicht die gleiche MAC-Adresse.

- **Gefälschte Übertragungen** – In der Standardeinstellung ist diese Option auf **Akzeptieren** gesetzt, d. h. der ESX Server-Host vergleicht die Quell- und die geltende MAC-Adresse nicht. Die Einstellungen der Option **Gefälschte Übertragungen** ändert den Datenverkehr, der von einer virtuellen Maschine versandt wird.

  Zum Schutz gegen MAC-Imitation können Sie diese Option auf **Reject** (Ablehnen) setzen. In diesem Fall vergleicht der ESX Server-Host die Quell-MAC-Adresse, die vom Betriebssystem übertragen wird, mit der geltenden MAC-Adresse des Adapters, um festzustellen, ob sie übereinstimmen. Wenn die Adressen nicht passen, verwirft der ESX Server das Paket.

  Das Gast-Betriebssystem erkennt nicht, dass der virtuelle Netzwerkadapter die Pakete mit der imitierten MAC-Adresse nicht senden kann. Der ESX Server-Host fängt alle Pakete mit imitierten Adressen vor der Auslieferung ab. Das Gast-Betriebssystem geht ggf. davon aus, das die Pakete verworfen wurden.

- **Betrieb im Promiscuous-Modus** – In der Standardeinstellung ist diese Option auf **Ablehnen** gesetzt, d. h. der virtuelle Netzwerkadapter kann nicht im Promiscuous-Modus betrieben werden. Der Promiscuous-Modus deaktiviert jegliche Empfangsfilterung, die der virtuelle Netzwerkadapter normalerweise ausführen würde, sodass das Gast-Betriebssystem den gesamten Datenverkehr aus dem Netzwerk empfängt.

  Zwar kann der Promiscuous-Modus für die Beobachtung der Netzwerkaktivitäten nützlich sein, aber er ist ein unsicherer Betriebsmodus, da jeder Adapter im Promiscuous-Modus Zugriff auf alle Pakete hat, auch wenn manche Pakete nur für einen spezifischen Netzwerkadapter bestimmt sind. Das bedeutet, dass ein Administrator oder Root-Anwender in einer virtuellen Maschine rein theoretisch den Datenverkehr, der für andere Gast- oder Hostbetriebssysteme bestimmt ist, einsehen kann.

HINWEIS Unter bestimmten Umständen ist es notwendig, einen virtuellen Switch in den Promiscuous-Modus zu setzen – zum Beispiel, wenn Sie eine Software zur Netzwerkeinbruchserkennung oder einen Paketmitschneider verwenden.

Wenn Sie eine dieser Standardeinstellungen für einen Port ändern möchten, müssen Sie das Sicherheitsprofil in den Einstellungen des virtuellen Switches im VI Client ändern. Informationen zum Bearbeiten dieser Einstellungen finden Sie unter „Policys für virtuelle Switches“ auf Seite 53.

Absicherung von iSCSI-Speicher

Zu dem Speicher, den Sie für einen ESX Server-Host konfigurieren, gehören ggf. Speichernetzwerke (SANs), die iSCSI verwenden. iSCSI dient zum Zugriff auf SCSI-Geräte und zum Austausch von Datenberichten unter Verwendung von TCP/IP über einen Netzwerkport statt über eine direkte Verbindung mit dem SCSI-Gerät. In iSCSI-Übertragungen werden Raw-SCSI-Datenblöcke in iSCSI-Berichte eingekapselt und an das Gerät oder den Anwender, der die Anfrage gestellt hat, übertragen.

iSCSI-SANs ermöglichen die effiziente Verwendung bestehender Ethernet-Infrastrukturen zum Zugriff auf Speicherressourcen durch die ESX Server-Hosts, die diese Ressourcen dynamisch teilen können. Als solche bieten iSCSI-SANs eine wirtschaftliche Speicherlösung für Umgebungen, die auf einem gemeinsamen Speicherpool für verschiedene Anwender basieren. Wie in allen vernetzten Systemen sind auch iSCSI-SANs anfällig für Sicherheitsbedrohungen. Wenn Sie iSCSI auf einem ESX Server-Host konfigurieren, können Sie diese Sicherheitsrisiken durch verschiedene Maßnahmen minimieren.

HINWEIS Die Anforderungen und Vorgehensweisen für die Absicherung von iSCSI-SANs ähneln denen für Hardware-iSCSI-Adapter, die Sie für ESX Server-Hosts und für iSCSI, das direkt über den ESX Server-Host konfiguriert wird, verwenden. Weitere Informationen zur Konfiguration von iSCSI-Adaptern und Speichern finden Sie unter „iSCSI-Speicher“ auf Seite 110.

Im folgenden Abschnitt wird beschrieben, wie Sie die Authentifizierung für iSCSI-SANs konfigurieren und wie Sie iSCSI-SANs absichern können. In diesem Abschnitt werden folgende Themen behandelt:

- „Absicherung von iSCSI-Geräten über Authentifizierung“ auf Seite 204
- „Schutz eines iSCSI-SANs“ auf Seite 208

Absicherung von iSCSI-Geräten über Authentifizierung

iSCSI-Geräten können gegen ungewollten Zugriff abgesichert werden, indem der ESX Server-Host (der *Initiator*), vom iSCSI-Gerät (dem *Ziel*) authentifiziert werden muss, wenn der Host versucht, auf Daten in der Ziel-LUN zuzugreifen. Ziel der Authentifizierung ist es zu überprüfen, dass der Inititator das Recht hat, auf ein Ziel zuzugreifen. Dieses Recht wird bei der Konfiguration der Authentifizierung gewährt.

Sie haben zwei Möglichkeiten, wenn Sie die Authentifizierung für iSCSI-SANs auf dem ESX Server-Host einrichten:

- **Challenge Handshake Authentication Protocol (CHAP)** – Sie können den iSCSI-SAN so konfigurieren, dass er CHAP-Authentifizierung verwendet. Bei der CHAP-Authentifizierung sendet das iSCSI-Ziel, wenn der Initiator mit ihm Kontakt aufnimmt, einen vordefinierten ID-Wert und einen Zufallswert, den *Schlüssel*, an den Initiator. Der Initiator erstellt dann einen Einweg-Prüfsummen-

wert, den er an das Ziel sendet. Die Prüfsumme enthält drei Elemente: einen vordefinierten ID-Wert, den Zufallswert, den das Ziel gesendet hat, und einen privaten Wert, den sog. *CHAP-Schlüssel*, den sowohl der Initiator als auch das Ziel haben. Wenn das Ziel die Prüfsumme vom Inititator erhält, erstellt es aus den gleichen Elementen seine eigene Prüfsumme und vergleicht diese mit dem Prüfsummenwert des Initiators. Wenn die Ergebnisse übereinstimmen, authentifiziert das Ziel den Initiator.

ESX Server unterstützt die Einweg-CHAP-Authentifizierung für iSCSI. Er unterstützt keine bidirektionale CHAP. Bei der Einweg-CHAP-Authentifizierung authentifiziert das Ziel den Initiator, nicht jedoch der Initiator das Ziel. Der Initiator verfügt nur über eine Identifikation, die von allen iSCSI-Zielen verwendet wird.

ESX Server unterstützt die CHAP-Authentifizierung nur auf HBA-Ebene. Die zielbasierte CHAP-Authentifizierung, bei der verschiedene Identifikationen für die Ziele erstellt werden können, um eine bessere Zielunterscheidung vornehmen zu können, wird nicht unterstützt.

- **Deaktiviert** – Sie können das iSCSI-SAN so konfigurieren, dass keine Authentifizierung verwendet wird. Beachten Sie, dass der Datenverkehr zwischen Initiator und Ziel dennoch rudimentär überprüft wird, da iSCSI-Zielgeräte normalerweise so eingerichtet sind, dass sie nur mit bestimmten Initiatoren kommunizieren.

  Die Deaktivierung einer strengeren Authentifizierung kann zum Beispiel sinnvoll sein, wenn sich der iSCSI-Speicher an einem Standort befindet und ein dediziertes Netzwerk oder VLAN für alle iSCSI-Geräte erstellt wird. Die Prämisse ist hier, dass die iSCSI-Konfiguration sicher ist, weil sie von ungewolltem Zugriff isoliert ist, wie dies auch in einem Fibre-Channel-SAN der Fall wäre.

  Deaktivieren Sie die Authentifizierung grundsätzlich nur dann, wenn Sie einen Angriff auf das iSCSI-SAN riskieren können oder Probleme beheben müssen, die durch menschliches Versagen entstanden sind.

ESX Server unterstützt für iSCSI weder Kerberos noch Secure Remote Protocol (SRP) noch Authentifizierungsverfahren mit öffentlichen Schlüsseln. Außerdem unterstützt es keine IPsec-Authentifizierung und -Verschlüsselung.

Mit dem VI Client können Sie bestimmen, ob die Authentifizierung derzeit verwendet wird, sowie zur Konfiguration der Authentifizierungsverfahren.

Überprüfung des Authentifizierungsverfahrens

1 Melden Sie sich am VI Client an und wählen Sie den Server aus dem Inventar aus.

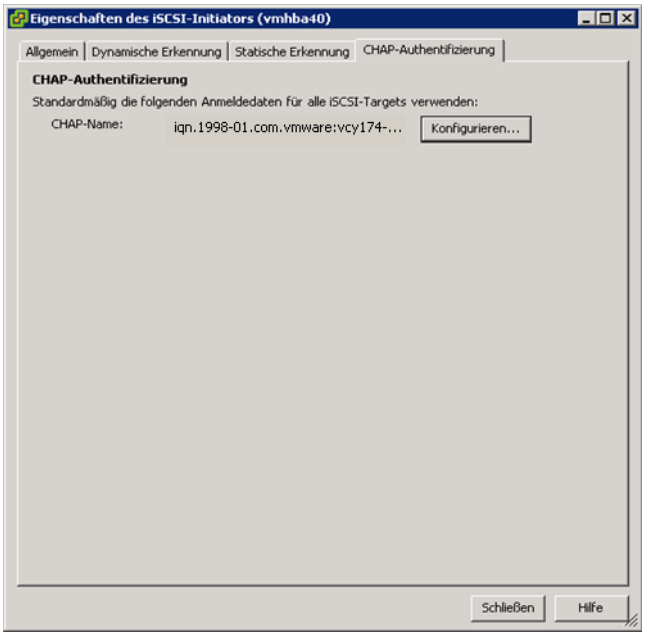
  Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Speicheradapter**.

3 Markieren Sie den gewünschten iSCSI-Adapter und klicken Sie dann auf **Eigenschaften**. Das Dialogfeld **Eigenschaften des iSCSI-Initiators** wird geöffnet.

4 Klicken Sie auf **CHAP Authentication** (CHAP-Authentifizierung).

Wenn unter **CHAP-Name** ein Name angezeigt wird–normalerweise der CHAP-Initiatorname, verwendet das iSCSI-SAN die CHAP-Authentifizierung (s.u.).



HINWEIS Wenn unter **CHAP Name** (CHAP-Name) **Not Specified** (Nicht festgelegt) angezeigt wird, verwendet das iSCSI-SAN die CHAP-Authentifizierung nicht.

5 Klicken Sie auf **Schließen**.

Konfiguration von iSCSI für die CHAP-Authentifizierung

1 Melden Sie sich am VI Client an und wählen Sie den Server aus dem Inventar aus.

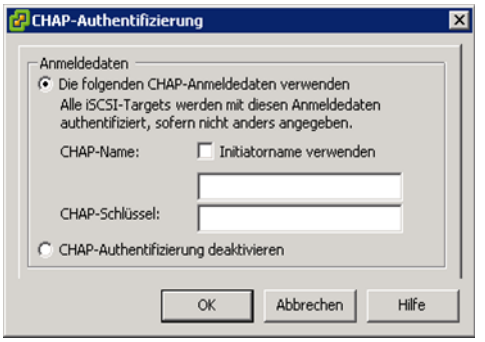
Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte Konfiguration und dann auf **Speicheradapter**.

3 Markieren Sie den gewünschten iSCSI-Adapter und klicken Sie dann auf **Eigenschaften**. Das Dialogfeld **Eigenschaften des iSCSI-Initiators** wird geöffnet.

4 Klicken Sie auf **CHAP-Authentifizierung** > **Konfigurieren**. Das Dialogfeld **CHAP-Authentifizierung** wird geöffnet.

5 Klicken Sie auf **Folgende CHAP-Identifikatoren verwenden**.



6 Führen Sie einen der folgenden Schritte aus:

- Wenn der CHAP-Name dem iSCSI-Adapternamen entsprechen soll, aktivieren Sie das Kontrollkästchen **Initiatornamen verwenden**.
- Um den CHAP-Name nicht mit dem iSCSI-Adapternamen zu vergeben, dürfen Sie **Initiatornamen verwenden** nicht auswählen und müssen stattdessen einen Namen von bis zu 255 alphanumerischen Zeichen im Feld **CHAP-Name** eingeben.

7 Geben Sie einen CHAP-Schlüssel ein, der als Teil der Authentifizierung verwendet werden soll.

Der Schlüssel, den Sie eingeben, ist eine Zeichenfolge.

HINWEIS Der VI Client verlangt keine Mindest- oder Höchstlänge für den CHAP-Schlüssel, den Sie eingeben. Bestimmte iSCSI-Speichergeräte fordern jedoch eine Mindestlänge oder beschränken die Art der verwendbaren Zeichen. Weitere Informationen zu den Anforderungen der Speichergeräte erhalten Sie in der Dokumentation des Herstellers.

---

8 Klicken Sie auf **OK**.

Deaktivierung der iSCSI-Authentifizierung

1 Melden Sie sich am VI Client an und wählen Sie den Server aus dem Inventar aus.

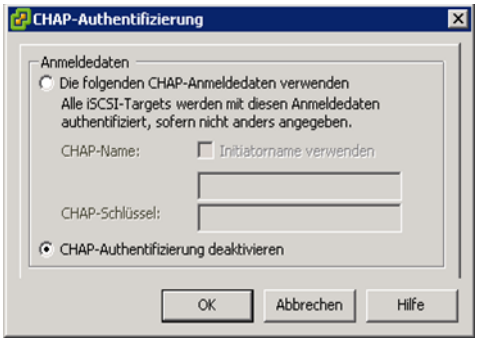
Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte Konfiguration und dann auf **Speicheradapter**.

3 Markieren Sie den gewünschten iSCSI-Adapter und klicken Sie dann auf **Eigenschaften**. Das Dialogfeld **Eigenschaften des iSCSI-Initiators** wird geöffnet.

4 Klicken Sie auf **CHAP-Authentifizierung** > **Konfigurieren**. Das Dialogfeld **CHAP-Authentifizierung** wird geöffnet.

5 Aktivieren Sie das Kontrollkästchen **CHAP-Authentifizierung deaktivieren**.



6 Klicken Sie auf **OK**.

Schutz eines iSCSI-SANs

Bei der Planung der iSCSI-Konfiguration sollten Sie Maßnahmen zur Verbesserung der allgemeinen Sicherheit des iSCSI-SANs ergreifen. Die iSCSI-Struktur ist nur so sicher wie das IP-Netzwerk – wenn Sie also hohe Sicherheitsstandards bei der Netzwerkeinrichtung umsetzen, schützen Sie auch den iSCSI-Speicher.

Hier sind einige spezifische Vorschläge zur Absicherung:

- **Schutz übertragener Daten** – Eines der Hauptrisiken bei iSCSI-SANs ist, dass der Angreifer übertragene Speicherdaten mitschneiden kann.

  VMware empfiehlt, dass Sie zusätzliche Maßnahmen ergreifen, um zu verhindern, dass Angreifer iSCSI-Daten sehen können. Weder der Hardware-iSCSI-Adapter noch der ESX Server-Host, d. h. der iSCSI-Initiator, verschlüsseln Daten, die von den und auf die Ziele übertragen werden, wodurch die Daten anfälliger für Abhörversuche sind.

  Wenn die virtuellen Maschinen die gleichen virtuellen Switches und VLANs wie die iSCSI-Struktur verwenden, ist der iSCSI-Datenverkehr potenziell dem Missbrauch durch Angreifer der virtuellen Maschinen ausgesetzt. Um sicherzustellen, dass Angreifer die iSCSI-Übertragungen nicht abhören können, achten Sie darauf, dass keine Ihrer virtuellen Maschinen das iSCSI-Speichernetzwerk sehen kann.

  Wenn Sie einen Hardware-iSCSI-Adapter verwenden, erreichen Sie dies, indem Sie sicherstellen, dass der iSCSI-Adapter und der ESX physische Netzwerkadapter nicht versehentlich außerhalb des Hosts durch eine gemeinsame Verwendung des Switch oder in anderer Form verbunden sind. Wenn Sie iSCSI direkt über den ESX Server-Host konfigurieren, können Sie dies erreichen, indem Sie den iSCSI-Speicher über

einen anderen virtuellen Switch konfigurieren, als denjenigen, der durch Ihre virtuellen Maschinen verwendet wird, wie in Abbildung 10-5 dargestellt.

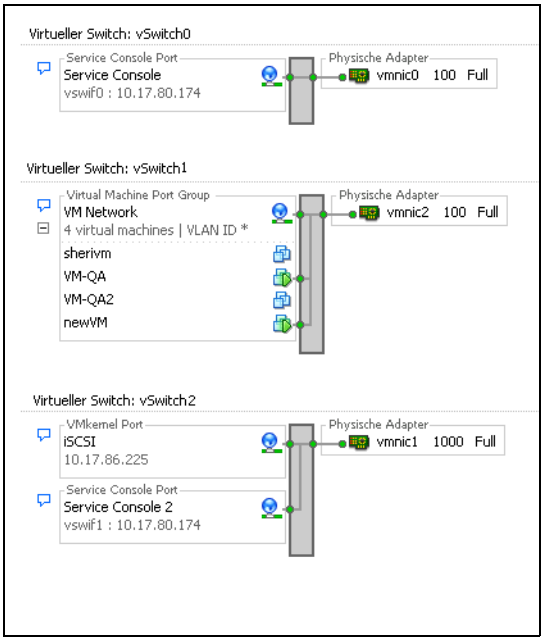


Abbildung 10-5. iSCSI-Speicher an einem eigenen virtuellen Switch

Wenn Sie iSCSI direkt durch den Host und nicht durch den Hardware-Adapter konfigurieren, müssen Sie beim Einrichten des virtuellen Netzwerks zwei Netzwerkverbindungen für die Servicekonsole anlegen. Dazu konfigurieren Sie die erste Netzwerkverbindung der Servicekonsole auf deren eigenem virtuellen Switch und verwenden diese ausschließlich für die Konnektivität der Management-Tools (*virtueller Switch 0* in der Abbildung). Dann konfigurieren Sie die zweite Netzwerkverbindung für die Servicekonsole, damit sie den virtuellen Switch verwendet, den Sie für die iSCSI-Konnektivität nutzen (*virtueller Switch 2* in der Abbildung). Die zweite Servicekonsolen-Netzwerkverbindung unterstützt nur die iSCSI-Aktivitäten und Sie sollten Sie nicht für Management-Aktivitäten oder die Management-Tool-Kommunikation verwenden. Wenn Sie eine gewisse Trennung zwischen iSCSI und der Servicekonsole auf dem gemeinsam genutzten virtuellen Switch herstellen möchten, können Sie sie auf unterschiedlichen VLANs konfigurieren.

HINWEIS Konfigurieren Sie nicht den Standard-Gateway für die Servicekonsole auf dem virtuellen Switch, den Sie für die iSCSI-Konnektivität verwenden. Konfigurieren Sie ihn stattdessen auf dem virtuellen Switch, den Sie für die Konnektivität der Management-Tools verwenden.

Zusätzlich zum Schutz durch einen eigenen virtuellen Switch können Sie das iSCSI-SAN durch die Konfiguration eines eigenen VLANs für das iSCSI-SAN schützen. Wenn die iSCSI-Struktur sich in einem eigenen VLAN befindet, wird sichergestellt, dass keine Geräte außer dem iSCSI-Adapter Einblick in Übertragungen im iSCSI-SAN haben.

- **Sicherung der iSCSI-Port** – Wenn Sie die iSCSI-Geräte ausführen, öffnet der ESX Server-Host keine Ports, die Netzwerkverbindungen abhören. Dadurch wird die Chance, dass ein Angreifer über ungenutzte Ports in den ESX Server-Host einbrechen und Kontrolle über ihn erlangen kann. Daher stellt der Betrieb von iSCSI kein zusätzliches Sicherheitsrisiko für den ESX Server-Host dar.

  Beachten Sie, dass auf jedem iSCSI-Zielgerät mindestens ein freigebener Port für iSCSI-Verbindungen vorhanden sein muss. Wenn es Sicherheitsprobleme in der Software des iSCSI-Gerätes gibt, können die Daten unabhängig von ESX Server in Gefahr sein. Installieren Sie alle Sicherheitspatches des Speicherherstellers und beschränken Sie die Anzahl der an das iSCSI-Netzwerk angeschlossenen Geräte, um dieses Risiko zu verringern.

Authentifizierung und Anwender-Management 11

In diesem Kapitel wird erläutert, wie ESX Server die Anwenderauthentifizierung vornimmt und wie Sie Anwender- und Gruppenzugriffsberechtigungen einrichten. Außerdem werden die Verschlüsselung für Verbindungen zum VI Client, zu SDK und zu VI-Web Access sowie die Konfigurierung eines delegierten Anwendernamens für Übertragungen bei NFS-Speichern erläutert.

In diesem Kapitel werden folgende Themen behandelt:

- „Absichern von ESX Server über Authentifizierung und Zugriffsberechtigungen“ auf Seite 211
- „Verschlüsselungs- und Sicherheitszertifikate für ESX Server“ auf Seite 228
- „Delegierte der virtuellen Maschine für NFS-Speicher“ auf Seite 234

Absichern von ESX Server über Authentifizierung und Zugriffsberechtigungen

ESX Server verwendet die PAM-Struktur (Pluggable Authentication Modules) zur Authentifizierung, wenn Anwender mit VirtualCenter, VI-Web Access oder der Servicekonsole auf den ESX Server-Host zugreifen. Die PAM-Konfiguration für VMware Dienste befindet sich unter `/etc/pam.d/vmware-authd`, in der die Verzeichnispfade zu Authentifizierungsmodulen gespeichert sind.

Die Standardinstallation von ESX Server verwendet wie Linux die `/etc/passwd`-Authentifizierung, Sie können ESX Server jedoch aus so konfigurieren, dass es eine andere verteilte Authentifizierungsmethode verwendet. Wenn Sie statt der Standardimplementation von ESX Server ein Authentifizierungsprogramm von Drittanbietern verwenden möchten, finden Sie Anleitungen dazu in der Dokumentation des entsprechenden Anbieters. Gegebenenfalls müssen Sie während der Einrichtung der Authentifizierung von Drittanbietern die Datei `/etc/pam.d/vmware-authd` mit neuen Modulinformationen aktualisieren.

Jedes Mal, wenn der VI Client oder ein Benutzer des VirtualCenters sich mit dem ESX Server-Host verbindet, startet der `sinnet` Prozess eine Instanz des VMware Authentifizierungs-Daemon (`vmware-authd`), der als Proxy dazu verwendet wird, Informationen aus dem VMware Host-Agenten zu versenden oder jenem zuzustellen (`VMware-Host`). Der `vmware-authd` Prozess empfängt einen ankommenden Verbindungsversuch und leitet ihn weiter zum `VMware-Host`-Prozess, der den Benutzernamen und das Kennwort des Clients empfängt und diese zum PAM-Modul für die Authentifizierung weiterleitet.

Abbildung 11-1 zeigt das Grundprinzip, wie ESX Server Übertragungen vom VI Client authentifiziert.

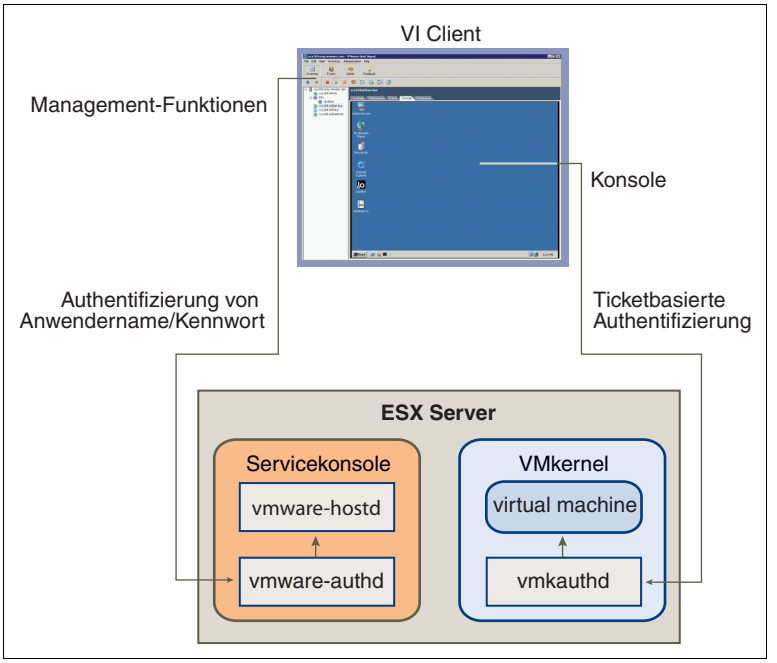


Abbildung 11-1. Authentifizierung für VI Client-Datenverkehr mit ESX Server

Der Prozess `vmware-authd` wird sofort beendet, wenn eine Verbindung zu einem VMware Prozess wie `vmware-hostd` hergestellt wurde. Alle Authentifizierungsprozesse virtueller Maschinen werden beendet, wenn der letzte Anwender die Verbindung trennt.

ESX Server-Übertragungen mit VI-Web Access und Netzwerk-Management-Clients von Drittanbietern interagieren während der Authentifizierung direkt mit dem Prozess `vmware-hostd`. Diese Verwaltungs-Tools umgehen `vmware-authd`.

Damit die Authentifizierung an Ihrem Standort effizient funktioniert, müssen Sie gegebenenfalls grundlegende Aufgaben wie die Einrichtung von Anwendern, Gruppen, Zugriffsberechtigungen und Rollen vornehmen, die Anwenderattribute konfigurieren,

eigene Zertifikate erstellen, ggf. SSL einrichten usw. Weitere Informationen zu diesen Themen und Aufgaben finden Sie in diesem Abschnitt, der folgende Themengebiete umfasst:

- „Anwender, Gruppen, Zugriffsberechtigungen und Rollen“ auf Seite 213
- „Verwaltung von Anwendern und Gruppen auf ESX Server-Hosts“ auf Seite 219
- „Verschlüsselungs- und Sicherheitszertifikate für ESX Server“ auf Seite 228
- „Delegierte der virtuellen Maschine für NFS-Speicher“ auf Seite 234

Anwender, Gruppen, Zugriffsberechtigungen und Rollen

Der Zugriff auf einen ESX Server-Host und dessen Ressourcen wird dann gewährt, wenn sich ein bekannter Anwender mit den entsprechenden Zugriffsberechtigungen auf dem Host mit einem Kennwort anmeldet, das dem für den Anwender gespeicherten Kennwort entspricht. VirtualCenter verwendet ein ähnliches Verfahren, um Anwendern Zugriff zu gewähren. VirtualCenter und ESX Server-Hosts bestimmen die Zugriffsebene für einen Anwender anhand der Zugriffsberechtigungen, die dem Anwender zugewiesen wurden. So kann zum Beispiel ein Anwender die Berechtigung haben, virtuelle Maschinen auf einem Host zu erstellen, während ein anderer Anwender zwar die Berechtigung hat, virtuelle Maschinen hochzufahren, nicht jedoch, sie zu erstellen.

Die Kombination aus Anwendername, Kennwort und Zugriffsberechtigungen wird von VirtualCenter und ESX Server-Hosts dazu verwendet, Anwender für den Zugriff zu authentifizieren und sie zur Ausführung bestimmter Tätigkeiten zu autorisieren. Dazu unterhalten VirtualCenter und der ESX Server-Host Verzeichnisse autorisierter Anwender mit ihren Kennwörtern und den ihnen zugewiesenen Zugriffsberechtigungen. VirtualCenter und ESX Server-Hosts verweigern den Zugriff unter folgenden Umständen:

- Ein Anwender, der nicht im Anwenderverzeichnis aufgeführt wird, versucht sich anzumelden.
- Ein Anwender gibt ein falsches Kennwort ein.
- Ein Anwender ist im Verzeichnis aufgeführt, ihm wurden jedoch keine Zugriffsberechtigungen zugewiesen.
- Ein Anwender, der sich erfolgreich angemeldet hat, versucht Vorgänge auszuführen, für die er keine Berechtigung besitzt.

Zur Verwaltung von ESX Server-Hosts und VirtualCenter gehört auch die Entwicklung von Anwender- und Berechtigungsmodellen, d. h. Grundplänen zur Behandlung bestimmter Anwenderarten und zur Zuweisung der Zugriffsberechtigungen. Beachten Sie bei der Entwicklung von Anwender- und Berechtigungsmodellen Folgendes:

- ESX Server und VirtualCenter verwenden Privilegiengruppen, sog. *Rollen*, um zu steuern, welche Vorgänge bestimmte Anwender oder Gruppen ausführen dürfen.

ESX Server und VirtualCenter verfügen über verschiedene vordefinierte Rollen, Sie können jedoch auch neue Rollen erstellen.

- Sie können Anwender einfacher verwalten, wenn Sie sie in Gruppen einteilen. Wenn Sie Gruppen erstellen, können Sie eine Rolle auf die Gruppe anwenden, die dann von allen Anwendern in dieser Gruppe übernommen wird.

Grundlegendes zu Anwendern

Ein Anwender ist eine Person, die sich am ESX Server-Host oder in VirtualCenter anmelden darf. Es gibt zwei Kategorien von ESX Server-Anwendern: Anwender, die über VirtualCenter auf den ESX Server-Host zugreifen, und Anwender, die direkt auf den ESX Server-Host zugreifen, indem Sie sich über den VI Client, VI-Web Access, Clients von Drittanbietern oder die Befehlszeile anmelden. Die Anwender in diesen beiden Kategorien haben folgenden Hintergrund.

- **VirtualCenter-Anwender** – Autorisierte Anwender für VirtualCenter sind die Anwender, die in der Windows-Domänenliste von VirtualCenter aufgeführt sind, oder lokale Windows-Anwender auf dem VirtualCenter-Host.

  Mit VirtualCenter können Sie Anwender nicht erstellen, entfernen oder anderweitig ändern. Um das Anwenderverzeichnis oder Anwenderkennwörter zu ändern, müssen Sie die Programme verwenden, mit denen Sie die Windows-Domäne verwalten.

  Alle Änderungen, die Sie in der Windows-Domäne vornehmen, werden in VirtualCenter widergespiegelt. Da Sie jedoch die Anwender nicht direkt in VirtualCenter verwalten können, enthält die Anwenderoberfläche auch kein Anwenderverzeichnis, das angezeigt werden kann. Nur bei der Auswahl von Anwendern und Gruppen während der Rollenzuweisung stehen Anwender- und Gruppenverzeichnisse zur Verfügung. Diese Änderungen machen sich nur bemerkbar, wenn Sie Anwender auswählen, um deren Zugriffsberechtigungen zu konfigurieren.

- **Anwender mit direktem Zugriff** – Anwender, die direkt auf einem ESX Server-Host arbeiten dürfen, sind die Anwender, die automatisch bei der Installation oder später vom Systemadministrator zur internen Anwenderliste hinzugefügt werden.

  Wenn Sie sich auf dem Host als Administrator anmelden, können Sie verschiedene Management-Aktivitäten für diese Anwender ausführen, z. B. Kennwörter, Gruppenmitgliedschaft, Zugriffsberechtigungen usw. ändern. Sie können diese Anwender auch hinzufügen oder entfernen.

Die von VirtualCenter geführte Anwenderliste ist eine grundlegend andere als die Anwenderliste des ESX Server-Hosts. Selbst wenn die Anwenderlisten von Host und VirtualCenter die gleichen Anwender zu haben scheinen (zum Beispiel einen Anwender mit dem Namen *devuser*), sollten diese Anwender als verschiedene Anwender behandelt werden, die zufällig den gleichen Namen haben. Die Attribute von *devuser* in VirtualCenter wie Zugriffsberechtigungen, Kennwörter usw. sind von den Attributen

von *devuser* auf dem ESX Server-Host getrennt. Wenn Sie sich im VirtualCenter als *devuser* anmelden, können Sie z. B. über die Berechtigung verfügen, Dateien aus einem Datastore anzusehen und zu löschen, was nicht der Fall sein muss, wenn Sie sich auf dem ESX Server-Host als *devuser* anmelden.

Aufgrund der Verwirrung, die doppelte Namen stiften können, empfiehlt VMware, dass Sie vor der Erstellung von ESX Server-Host-Anwendern das Anwenderverzeichnis von VirtualCenter überprüfen, um zu vermeiden, dass Sie Host-Anwender erstellen, die den gleichen Namen wie VirtualCenter-Anwender haben. Das Verzeichnis der VirtualCenter-Anwender finden Sie im Windows-Domänenverzeichnis.

Grundlegendes zu Gruppen

Bestimmte Anwenderattribute können Sie effektiver verwalten, indem Sie Gruppen erstellen. Eine Gruppe ist eine Ansammlung von Anwendern, die durch gemeinsame Regeln und Berechtigungen verwaltet werden sollen. Wenn Sie einer Gruppe Zugriffsberechtigungen zuweisen, werden diese von allen Anwendern in der Gruppe übernommen, wodurch Sie die Anwenderprofile nicht einzeln bearbeiten müssen. Daher kann die Verwendung von Gruppen die Zeit zur Implementierung des Berechtigungsmodells wesentlich verkürzen und zukunftsorientiert die Skalierbarkeit verbessern.

Als Administrator müssen Sie entscheiden, wie die Gruppen strukturiert werden sollen, um die Sicherheits- und Verwendungsziele zu erreichen. Sie haben zum Beispiel drei Teilzeitangestellte in der Verkaufsabteilung, die an verschiedenen Tagen arbeiten und zwar auf eine bestimmte virtuelle Maschine zugreifen sollen, nicht jedoch auf die virtuellen Maschinen des Verkaufsleiters. In diesem Fall können Sie eine Gruppe, z. B. *VerkaufTeilzeit* einrichten, zu der diese drei Teilzeitangestellten gehören: *Maria*, *Thomas* und *Peter*. Sie können dann der Gruppe *VerkaufTeilzeit* die Berechtigung zur Interaktion mit nur einem Objekt, der *virtuellen Maschine A*, zuweisen. *Maria*, *Thomas* und *Peter* übernehmen diese Zugriffsberechtigungen und können die *virtuelle Maschine A* hochfahren, Konsolensitzungen auf der *virtuellen Maschine A* aufrufen usw. Sie können diese Vorgänge jedoch nicht auf den virtuellen Maschinen des Verkaufsleiters durchführen: den *virtuellen Maschinen B*, *C* und *D*.

Die Gruppenverzeichnisse in VirtualCenter und auf dem ESX Server-Host stammen aus den gleichen Quellen wie die entsprechenden Anwenderverzeichnisse. Wenn Sie mit VirtualCenter arbeiten, wird das Gruppenverzeichnis von der Windows-Domäne abgerufen. Wenn Sie sich direkt am ESX Server-Host angemeldet haben, wird das Gruppenverzeichnis aus einer Tabelle abgerufen, die vom Host erstellt wird. Die Empfehlungen zur Behandlung von Gruppenverzeichnissen entsprechen den Empfehlungen für Anwenderverzeichnisse.

Grundlegendes zu Zugriffsberechtigungen

Für ESX Server und VirtualCenter werden Zugriffsberechtigungen als Zugriffsrollen definiert, die aus einem Anwender und der dem Anwender zugewiesenen Rolle für ein Objekt wie z. B. einer virtuellen Maschine oder einem ESX Server-Host bestehen. Zugriffsberechtigungen geben Anwendern das Recht, bestimmte Vorgänge auszuführen und bestimmte Objekte auf einem ESX Server-Host oder, wenn Anwender von VirtualCenter aus arbeiten, alle von VirtualCenter verwalteten Objekte zu verwalten. Wenn Sie zum Beispiel Speicher für einen ESX Server-Host konfigurieren möchten, müssen Sie über eine Berechtigung zur Host-Konfiguration verfügen.

Die meisten VirtualCenter- und ESX Server-Anwender können Objekte des Hosts nur in eingeschränktem Maße ändern. ESX Server gibt jedoch zwei Anwendern vollständige Zugriffsrechte und Berechtigungen für alle virtuellen Objekte wie z. B. Datastores, Hosts, virtuelle Maschinen und Ressourcen-Pools – dem Root und, wenn der Host durch VirtualCenter verwaltet wird, dem vpxuser. Root und vpxuser verfügen über folgende Berechtigungen:

- **root** – Der Root-Anwender kann auf dem ESX Server-Host, auf dem er sich angemeldet hat, alle Steuerungsvorgänge wie z. B. die Verwaltung von Zugriffsberechtigungen, die Erstellung von Gruppen und Anwendern, Ereignisverwaltung usw. vornehmen. Ein Root-Anwender, der auf einem ESX Server-Host angemeldet ist, kann jedoch die Aktivitäten anderer Hosts im ESX Server-System nicht beeinflussen.

  Aus Sicherheitsgründen möchten Sie vielleicht nicht den Root-Benutzer in der Administratorenrolle sehen. In diesem Fall können Sie die Genehmigungen nach der Installation so ändern, dass der Root-Anwender keine weiteren Administratorrechte hat oder Sie löschen alle Zugriffsrechte des Root-Anwenders über den VI Client, wie im Kapitel „Verwaltung der Benutzer, Gruppen, Berechtigungen und Rollen“ des *Handbuchs für Systemadministratoren* beschrieben. Wenn Sie dies tun, müssen Sie auf der Root-Ebene zunächst eine andere Genehmigung erteilen, die ein anderer Benutzer mit der Rolle des Administrators erhält.

  Die Zuweisung der Administratorenrolle auf verschiedene Anwender gewährleistet die Nachvollziehbarkeit und somit die Sicherheit. Der VI Client protokolliert alle Aktionen des Administrators als Ereignisse und gibt Ihnen ein Überwachungsprotokoll aus. Sie können diese Funktion zur Verbesserung der Verantwortlichkeiten der verschiedenen Anwender verwenden, die für einen Host als Administratoren handeln. Wenn alle Administratoren sich am Host als Root-Anwender anmelden, können Sie nicht wissen, welche Administrator eine Aktion ausgeführt hat. Wenn Sie jedoch mehrere Genehmigungen auf Root-Ebene anlegen – die jeweils einem anderen Anwender oder einer anderen Anwendergruppe zugewiesen sind – können Sie die Aktionen jedes Administrators oder jeder Administratorengruppe gut nachvollziehen.

Nachdem Sie einen alternativen Administrator-Benutzer angelegt haben, können Sie sicher die Genehmigungen des Root-Benutzers löschen oder dessen Rolle in der Form ändern, dass seine Rechte begrenzt werden. Wenn Sie die Berechtigungen der Root-Anwender löschen oder ändern, müssen Sie den neu erstellten Anwender als Anlaufstelle für die Host-Authentifizierung verwenden, wenn Sie den Host unter die Verwaltung von VirtualCenter stellen. Weitere Informationen zu Rollen finden Sie unter „Grundlegendes zu Rollen“ auf Seite 218.

HINWEIS Konfigurationsbefehle, die Sie über die Befehlszeilenoberfläche ausführen (`esxcfg`-Befehle), führen keine Zugriffsprüfung durch.

- **vpxuser** – Dieser Anwender ist VirtualCenter, das auf dem ESX Server-Host mit Administrator-Rechten agiert, wodurch es Vorgänge für diesen Host verwalten kann. Der vpxuser wird erstellt, wenn der ESX Server-Host an VirtualCenter angebunden wird. Diesen Anwender gibt es auf dem ESX Server-Host nur, wenn der Host über VirtualCenter verwaltet wird.

  Wenn ein ESX Server-Host über VirtualCenter verwaltet wird, hat VirtualCenter Privilegien auf diesem Host. So kann VirtualCenter zum Beispiel virtuelle Maschinen auf Hosts verschieben und Konfigurationsänderungen vornehmen, die für die Unterstützung von virtuellen Maschinen notwendig sind.

  Der Administrator von VirtualCenter kann über den vpxuser viele der Aufgaben des Root-Anwenders auf dem Host durchführen und Aufgaben planen, Vorlagen erstellen und nutzen usw. Es gibt jedoch bestimmte Vorgänge, die als VirtualCenter-Administrator nicht vorgenommen werden können. Diese Aktivitäten, zu denen die direkte Erstellung, Löschung oder Bearbeitung von Anwendern und Gruppen für ESX Server-Hosts gehören, können nur vom Anwender mit Administratoren-Genehmigungen direkt auf dem entsprechenden ESX Server-Host vorgenommen werden.

VORSICHT Ändern Sie den vpxuser und seine Berechtigungen nicht. Ansonsten kann es zu Problemen bei der Verwaltung des ESX Server-Hosts über VirtualCenter kommen.

Wenn Sie als Administrator an einem ESX Server Host angemeldet sind, können Sie einzelnen Anwendern oder Gruppen, die standardmäßig bei der Installation von ESX Server oder später manuell zum ESX Server-Anwender- bzw. Gruppenverzeichnis hinzugefügt wurden, Zugriffsberechtigungen für einen ESX Server-Host zuweisen. Wenn Sie als Administrator in VirtualCenter angemeldet sind, können Sie allen Anwendern oder Gruppen im von VirtualCenter übernommenen Windows-Domänenverzeichnis Berechtigungen zuweisen.

HINWEIS VirtualCenter registriert alle ausgewählten Anwender oder Gruppen der Windows-Domäne durch den Prozess der Zuweisung von Zugriffsberechtigungen. Standardmäßig werden allen Anwendern, die zur lokalen WindowsAdministratorengruppe auf dem VirtualCenter Server gehören, die gleichen Zugriffsrechte wie Anwendern mit Administratorenrolle zugewiesen. Anwender, die zur Administratorengruppe gehören, können sich einzeln anmelden und verfügen über vollständige Zugriffsrechte.

Das Verfahren zur Konfiguration von Zugriffsberechtigungen direkt auf einem ESX Server-Host entspricht dem Verfahren zur Konfiguration von Zugriffsberechtigungen in VirtualCenter. Auch die Liste der Privilegien ist auf ESX Server und in VirtualCenter gleich. Weitere Informationen zur Konfiguration von Zugriffsberechtigungen und zu den Privilegien, die zugewiesen werden können, finden Sie in der *Einführung in die virtuelle Infrastruktur*.

Grundlegendes zu Rollen

VirtualCenter und ESX Server gewähren Zugriff auf Objekte nur an die Anwender, denen Berechtigungen für ein Objekt zugewiesen wurden. Wenn Sie einem Anwender oder einer Gruppe Zugriffsberechtigungen für ein Objekt zuweisen, geschieht dies durch Zuweisung einer Rolle zum Anwender oder zu der Gruppe. Eine Rolle ist eine vordefinierte Sammlung von Privilegien.

Für ESX Server-Hosts gibt es drei Standardrollen. Es ist nicht möglich, die Privilegien für diese drei Rollen zu ändern. Jede nachfolgende Standardrolle enthält die Privilegien der vorhergehenden Rolle. So übernimmt beispielsweise die Administrator-Rolle die Rechte der Lesezugriff-Rolle. Rollen, die Sie selbst anlegen, übernehmen keine Rechte aus den Standardrollen. Es gibt folgende Standardrollen:

- **Kein Zugriff** – Anwender, denen diese Rolle für ein bestimmtes Objekt zugewiesen wurde, können das Objekt weder anzeigen noch ändern. So kann zum Beispiel ein Anwender, dem für eine bestimmte virtuelle Maschine die Rolle „Kein Zugriff“ zugewiesen wurde, die virtuelle Maschine nicht in der VI Client-Inventar sehen, wenn er oder sie sich auf dem ESX Server-Host anmeldet. Wenn einem Anwender für ein bestimmtes Objekt diese Rolle zugewiesen wurde, kann er oder sie die Registerkarten im VI Client für das verbotene Objekt auswählen, aber es wird kein Inhalt angezeigt. Wenn der Anwender zum Beispiel keinen Zugriff auf virtuelle Maschinen hat, kann er oder sie die Registerkarte „Virtual Machines (Virtuelle Maschinen)“ anklicken, aber er sieht weder das Verzeichnis der virtuellen Maschinen auf der Registerkarte noch die Statusinformationen – die Tabelle ist leer.

  Die Rolle „Kein Zugriff“ ist die Standardrolle, die allen Anwendern oder Gruppen, die Sie auf einem ESX Server-Host erstellen, zugewiesen wird. Sie können die Rolle neuer Anwender oder Gruppen objektabhängig mit höheren oder niedrigeren Zugriffsrechten ausstatten.

HINWEIS Die einzigen Anwender, denen die Rolle „Kein Zugriff“ nicht standardmäßig zugewiesen wird, sind der Root-Anwender und der vpxuser. Stattdessen wird ihnen die Administratorenrolle zugewiesen. Ändern Sie die Rolle für diese Anwender nicht.

Sie können die Genehmigungen der Root-Anwender insgesamt löschen oder deren Rolle auf „Kein Zugriff“ setzen, sofern Sie zunächst auf dem Rootlevel eine Ersatzgenehmigung mit der Administratorrolle anlegen und diese Rolle einem anderen Anwender zuweisen. Wenn Sie die Berechtigungen der Root-Anwender löschen oder ändern, müssen Sie den neu erstellten Anwender als Anlaufstelle für die Host-Authentifizierung verwenden, wenn Sie den Host unter die Verwaltung von VirtualCenter stellen.

- **Lesezugriff** – Anwender, denen diese Rolle für ein Objekt zugewiesen wurde, können den Status des Objekts und Details zum Objekt ansehen.

  In dieser Rolle kann ein Anwender die virtuelle Maschine, den Host und die Ressourcen-Pool-Attribute anzeigen lassen. Der Anwender kann jedoch nicht die Remote-Steuerung für einen Host einsehen. Alle Vorgänge über Menüs und Symbolleisten sind nicht zugelassen.

- **Administrator** – Anwender, denen diese Rolle für ein Objekt zugewiesen wurde, können alle Vorgänge auf dem Objekt anzeigen und durchführen. Zu dieser Rolle gehören alle Zugriffsberechtigungen, über die auch die Rolle mit Lesezugriff verfügt.

Anwenderdefinierte Rollen können Sie mit den Rollenbearbeitungsdienstprogrammen auf dem VI Client erstellen und an Ihre Bedürfnisse anpassen. Wenn Sie den VI Client über VirtualCenter zur Verwaltung der ESX Server-Hosts verwenden, stehen Ihnen zusätzliche Rollen im VirtualCenter zur Auswahl. Auf die Rollen, die Sie direkt auf einem ESX Server-Host erstellen, kann nicht von VirtualCenter aus zugegriffen werden. Sie können diese Rollen nur verwenden, wenn Sie sich direkt über den VI Client auf dem Host anmelden.

Wenn Sie ESX Server-Hosts über VirtualCenter verwalten, sollten Sie beachten, dass die Verwendung von anwenderdefinierten Rollen auf dem Host und im VirtualCenter zu Verwirrung und Missbrauch führen kann. Bei dieser Art der Konfiguration empfiehlt VMware, dass Sie nur anwenderdefinierte Rollen in VirtualCenter verwenden. Informationen zur Erstellung, Änderung und Löschung von Rollen sowie zu den zusätzlich in VirtualCenter verfügbaren Rollen finden Sie im *Handbuch zur Systemverwaltung*.

Verwaltung von Anwendern und Gruppen auf ESX Server-Hosts

Wenn Sie direkt über einen VI Client mit einem ESX Server-Host verbunden sind, können Sie Anwender und Gruppen erstellen, bearbeiten und löschen. Diese Anwender und Gruppen werden im VI Client angezeigt, wenn Sie sich auf dem ESX Server-Host anmelden, in VirtualCenter stehen Sie jedoch nicht zur Verfügung.

Im folgenden Abschnitt wird erläutert, wie Anwender und Gruppen in einem direkt an den ESX Server-Host angeschlossenen VI Client verwaltet werden können. Es werden die grundlegenden Aufgaben behandelt, die Sie für Anwender und Gruppen durchführen können, wie zum Beispiel die Anzeige und Sortierung von Informationen und der Export von Berichten. Es wird auch gezeigt, wie Anwender und Gruppen erstellt, bearbeitet und gelöscht werden können.

HINWEIS Sie können auch über eine direkte Verbindung mit dem ESX Server-Host Rollen erstellen und Zugriffsberechtigungen einrichten. Da diese Aufgaben in VirtualCenter in größerem Umfang und häufiger durchgeführt werden, finden Sie nähere Informationen zum Umgang mit Zugriffsberechtigungen und Rollen in der *Einführung in die virtuelle Infrastruktur*.

Anzeige und Export von Anwender- und Gruppeninformationen

Anwender und Gruppen werden über die Registerkarte **Anwender und Gruppen** im VI Client verwaltet. Diese Registerkarte zeigt die Tabelle **Anwender** oder die Tabelle **Gruppen**an, je nachdem, ob Sie auf die Schaltfläche **Anwender** oder **Gruppen** klicken.

Abbildung 11-2 zeigt die Tabelle **Anwender** an. Die Tabelle **Gruppen** sieht ähnlich aus.

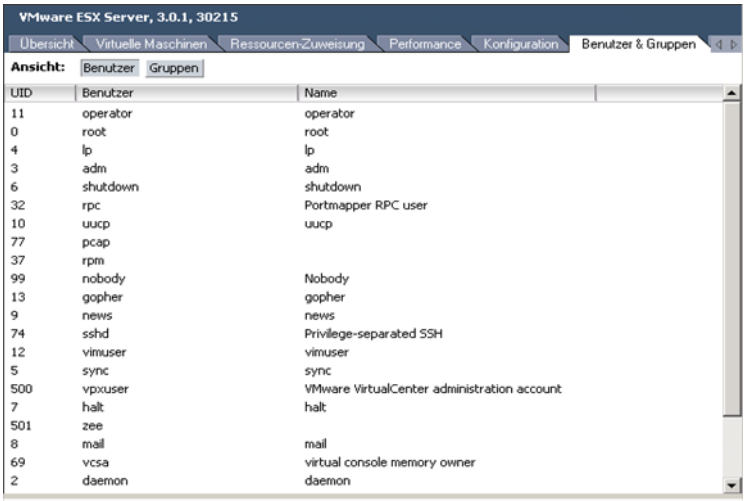


Abbildung 11-2. Anwendertabelle

Sie können die Verzeichnisse nach Spalten sortieren, Spalten ein- oder ausblenden und die Verzeichnisse in Formate exportieren, die Sie zur Erstellung von Berichten oder zur Veröffentlichung von Anwender- oder Gruppenverzeichnissen im Internet verwenden können.

Anzeigen und Sortieren von ESX Server-Anwendern oder -Gruppen

1 Melden Sie sich über den ESX Server-Host im VI Client an.

2 Wählen Sie den Server aus dem Inventar aus.

Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

3 Klicken Sie auf die Registerkarte **Anwender & Gruppen** und dann auf **Anwender** oder **Gruppen**.

4 Führen Sie je nach Bedarf folgende Schritte aus:

- Wenn Sie die Tabelle nach einer Spalte sortieren möchten, klicken Sie auf die entsprechende Spaltenüberschrift.
- Wenn Sie eine Spalte ein- oder ausblenden möchten, klicken Sie mit der rechten Maustaste auf eine der Spaltenüberschriften und aktivieren oder deaktivieren Sie den Namen der Spalte, die Sie ein- oder ausblenden möchten.

Datenexport aus der ESX Server-Anwender- oder Gruppentabelle

1 Melden Sie sich über den ESX Server-Host im VI Client an.

2 Wählen Sie den Server aus dem Inventar aus.

Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

3 Klicken Sie auf die Registerkarte **Anwender & Gruppen** und dann auf **Anwender** oder **Gruppen**.

4 Legen Sie die Sortierreihenfolge der Tabelle fest und blenden Sie Spalten ein oder aus, je nachdem, welche Daten in der Exportdatei enthalten sein sollen.

5 Klicken Sie mit der rechten Maustaste an eine beliebige Stelle in der Anwendertabelle und wählen Sie die Option **Exportieren.** Das Dialogfeld **Speichern unter** wird angezeigt.

6 Wählen Sie ein Verzeichnis aus und geben Sie einen Dateinamen ein.

7 Wählen Sie den Dateityp aus.

Folgende Exportformate stehen für Anwender- und Gruppentabellen zur Verfügung:

- HTML (normales HTML oder für die Verwendung bei CSS-Stylesheets formatiertes HTML)
- XML
- Microsoft Excel
- CSV (Kommagetrennte Werte)

8 Klicken Sie auf **OK**.

Verwaltung der Anwendertabelle

Sie können Anwender zur **Anwender**-Tabelle eines ESX Server-Hosts hinzufügen, Anwender entfernen und andere Attribute wie Kennwort und Gruppenmitgliedschaft ändern. Dabei ändern Sie das interne, vom ESX Server-Host erstellte Anwenderverzeichnis.

Hinzufügen eines Anwenders zu einer ESX Server-Anwendertabelle

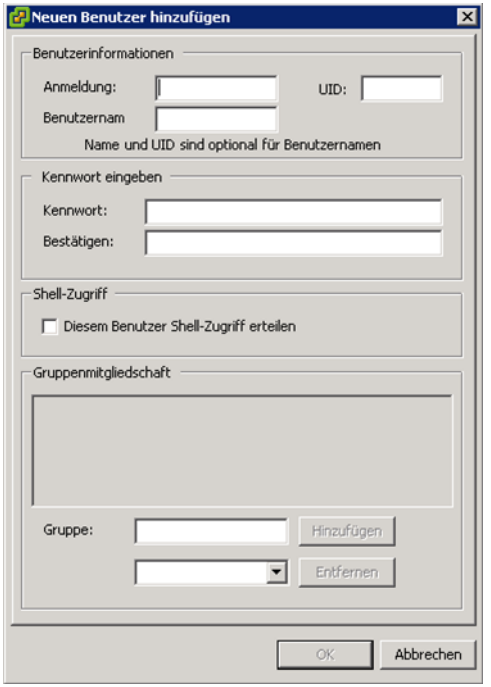
1 Melden Sie sich über den ESX Server-Host im VI Client an.

2 Wählen Sie den Server aus dem Inventar aus.

Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

3 Klicken Sie auf die Registerkarte **Anwender & Gruppen** und dann auf **Anwender**.

4 Klicken Sie mit der rechten Maustaste an eine beliebige Stelle in der Anwendertabelle und wählen Sie die Option **Hinzufügen**. Das Dialogfeld **Neuen Anwender hinzufügen** wird angezeigt.



5 Geben Sie eine Anmeldung, einen Benutzernamen, eine numerische Benutzer-ID (UID) und ein Kennwort ein.

Die Angabe des Benutzernamens und der UID sind rein optional. Wenn Sie keine UID angeben, weist der VI Client die nächste verfügbare UID zu.

Das Kennwort sollte in Länge und Komplexität den Anforderungen im Abschnitt „Kennwortbeschränkungen“ auf Seite 244 entsprechen. Der ESX Server-Host prüft nur dann auf eine Übereinstimmung des Kennworts, wenn Sie zum Plug-in `pam_passwdqc.so` gewechselt haben, um sich zu authentifizieren. Die Kennworteinstellungen im Standard-Authentifizierungs-Plug-In `pam_cracklib.so` werden nicht erzwungen.

6 Wenn der Anwender in der Lage sein soll, über eine Befehlsshell auf den ESX Server-Host zuzugreifen, aktivieren Sie das Kontrollkästchen **Zugriff über Befehlsshell für diesen Anwender zulassen**.

Im Allgemeinen sollte der Shellzugriff nur ESX Server-Host-Anwendern gewährt werden, die diesen Zugriff auf den Host über eine Shell statt über den VI Client tatsächlich benötigen. Anwender, die nur über den VI Client auf den Host zugreifen, benötigen keinen Shellzugriff.

7 Geben Sie die Gruppennamen der Gruppen ein, zu denen der Anwender gehören soll, und klicken Sie auf **Hinzufügen**.

Wenn Sie einen nicht vorhandenen Gruppennamen eingeben, gibt der VI Client eine Warnmeldung aus und fügt die Gruppe nicht zum Verzeichnis **Gruppenmitgliedschaft** hinzu.

8 Klicken Sie auf **OK**.

Das Login und der Anwendername, die Sie eingegeben haben, werden jetzt in der **Anwender**-Tabelle angezeigt. Der VI Client weist dem Anwender die nächste verfügbare Anwender-ID zu.

Änderung von Einstellungen eines Anwenders

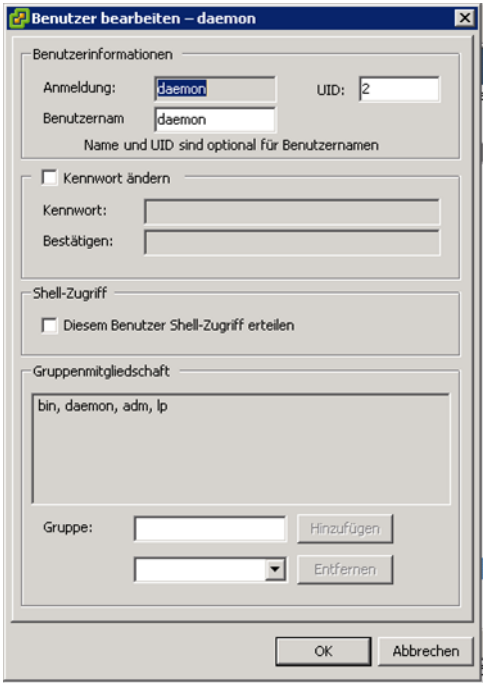
1 Melden Sie sich über den ESX Server-Host im VI Client an.

2 Wählen Sie den Server aus dem Inventar aus.

Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

3 Klicken Sie auf die Registerkarte **Anwender & Gruppen** und dann auf **Anwender**.

4 Klicken Sie mit der rechten Maustaste an eine beliebige Stelle in der Tabelle **Benutzer** und dann auf **Bearbeiten**. Das Dialogfeld **Anwender bearbeiten** wird angezeigt.



5 Wenn Sie die UID ändern möchten, geben Sie im Feld **UID** eine numerische UID ein.

Der VI Client weist einem Anwender bei seiner Erstellung die UID zu. In den meisten Fällen muss diese Zuweisung nicht geändert werden.

6 Geben Sie einen neuen Anwendernamen ein.

7 Wenn Sie das Kennwort eines Anwenders ändern möchten, aktivieren Sie das Kontrollkästchen **Kennwort ändern** und geben Sie ein neues Kennwort ein.

Das Kennwort sollte in Länge und Komplexität den Anforderungen im Abschnitt „Kennwortbeschränkungen“ auf Seite 244 entsprechen. Der ESX Server-Host prüft nur dann auf eine Übereinstimmung des Kennworts, wenn Sie zum Plug-in `pam_passwdqc.so` gewechselt haben, um sich zu authentifizieren. Die Kennworteinstellungen im Standard-Authentifizierungs-Plug-In `pam_cracklib.so` werden nicht erzwungen.

8 Um die Einstellung zu ändern, dass Anwender über eine Befehlsshell auf den ESX Server-Host zugreifen kann, aktivieren oder deaktivieren Sie das Kontrollkästchen **Anwender Shell-Zugriff gewähren**.

9 Wenn Sie den Anwender zu einer anderen Gruppe hinzufügen möchten, geben Sie den Gruppennamen ein und klicken Sie auf **Hinzufügen**.

Wenn Sie einen nicht vorhandenen Gruppennamen eingeben, gibt der VI Client eine Warnmeldung aus und fügt die Gruppe nicht zum Verzeichnis **Gruppenmitgliedschaft** hinzu.

10 Wenn Sie einen Anwender aus einer Gruppe entfernen möchten, wählen Sie den Gruppennamen aus dem Verzeichnis aus und klicken Sie auf **Entfernen**.

11 Klicken Sie auf **OK**.

Entfernen eines Anwenders aus der ESX Server-Anwendertabelle

1 Melden Sie sich über den ESX Server-Host im VI Client an.

2 Wählen Sie den Server aus dem Inventar aus.

Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

3 Klicken Sie auf die Registerkarte **Anwender & Gruppen** und dann auf **Anwender**.

4 Klicken Sie mit der rechten Maustaste auf den Anwender, den Sie entfernen möchten, und klicken Sie auf **Entfernen**.

VORSICHT Entfernen Sie **nicht** den Root-Anwender.

Verwaltung der Gruppentabelle

Sie können Gruppen zur **Gruppen**-Tabelle eines ESX Server-Hosts hinzufügen, Gruppen entfernen oder Gruppenmitglieder hinzufügen oder entfernen. Dabei ändern Sie das interne, vom ESX Server-Host erstellte Gruppenverzeichnis.

Hinzufügen einer Gruppe zur ESX Server-Gruppentabelle

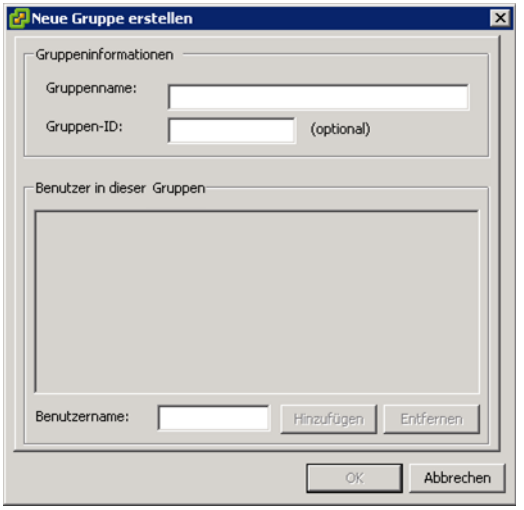
1 Melden Sie sich über den ESX Server-Host im VI Client an.

2 Wählen Sie den Server aus dem Inventar aus.

Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

3 Klicken Sie auf die Registerkarte **Anwender & Gruppen** und denn auf **Gruppen**.

4 Klicken Sie mit der rechten Maustaste an eine beliebige Stelle in der Tabelle **Gruppen** und dann auf **Hinzufügen**. Das Dialogfeld **Neue Gruppe erstellen** wird angezeigt.



5 Geben Sie einen Gruppennamen und eine numerische Gruppen-ID (GID) ein.

Die Angabe der GID ist nicht zwingend erforderlich. Wenn Sie keine GID angeben, weist der VI Client die nächste verfügbare GID zu.

6 Geben Sie die Anwendernamen aller Anwender ein, die zur Gruppe gehören sollen, und klicken Sie auf **Hinzufügen**.

Wenn Sie einen nicht vorhandenen Anwendernamen eingeben, gibt der VI Client eine Warnmeldung aus und fügt den Anwender nicht zum Verzeichnis **Gruppenmitglieder** hinzu.

7 Klicken Sie auf **OK**.

Die Gruppen-ID und der Gruppenname, den Sie eingegeben haben, werden jetzt in der **Gruppen**-Tabelle angezeigt.

Hinzufügen oder Entfernen von Gruppenanwendern

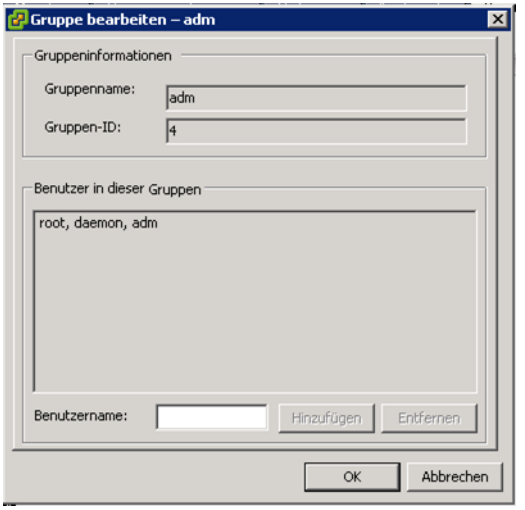
1 Melden Sie sich über den ESX Server-Host im VI Client an.

2 Wählen Sie den Server aus dem Inventar aus.

Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

3 Klicken Sie auf die Registerkarte **Anwender & Gruppen** und denn auf **Gruppen**.

4 Klicken Sie mit der rechten Maustaste an eine beliebige Stelle in der Tabelle **Gruppen** und dann auf **Eigenschaften.** Das Dialogfeld **Gruppe bearbeiten** wird angezeigt.



5 Wenn Sie einen Anwender zu einer Gruppe hinzufügen möchten, geben Sie den Anwendernamen ein und klicken Sie auf **Hinzufügen**.

Wenn Sie einen nicht vorhandenen Anwendernamen eingeben, gibt der VI Client eine Warnmeldung aus und fügt den Anwender nicht zum Verzeichnis **Gruppenmitglieder** hinzu.

6 Wenn Sie einen Anwender aus der Gruppe entfernen möchten, wählen Sie den Anwendernamen aus dem Verzeichnis aus und klicken Sie auf **Entfernen**.

7 Klicken Sie auf **OK**.

Entfernen einer Gruppe aus der ESX Server-Gruppentabelle

1 Melden Sie sich über den ESX Server-Host im VI Client an.

2 Wählen Sie den Server aus dem Inventar aus.

Die Seite „Hardware-Konfiguration“ für diesen Server wird angezeigt.

3 Klicken Sie auf die Registerkarte **Anwender & Gruppen** und denn auf **Gruppen**.

4 Klicken Sie mit der rechten Maustaste auf die Gruppe, die Sie entfernen möchten, und klicken Sie auf **Entfernen**.

VORSICHT Entfernen Sie die Root-Gruppe **nicht**.

Verschlüsselungs- und Sicherheitszertifikate für ESX Server

Der gesamte Netzwerkverkehr einschließlich Anwendernamen und Kennwörtern werden von VirtualCenter oder VI-Web Access über eine Netzwerkverbindung über Port 902 oder 443 an einen ESX Server-Host gesendet und standardmäßig von ESX Server verschlüsselt, wenn folgende Bedingungen vorliegen:

- SSL ist aktiviert.
- Der Web-Proxy-Dienst wurde nicht geändert, sodass er unverschlüsselten Datenverkehr für den Port durchlässt.
- Bei der Firewall der Servicekonsole wurde mittlere oder hohe Sicherheit eingestellt. Informationen zur Konfiguration der Firewall der Servicekonsole finden Sie unter „Konfiguration der Servicekonsolen-Firewall“ auf Seite 240.

VORSICHT Wenn Sie die Firewall deaktivieren, indem Sie den Modus „Niedrige Sicherheit“ einstellen, können die Anwender über den unsicheren Port 8080 auf den ESX Server-Host zugreifen. Jeder, der über Port 8080 auf den ESX Server-Host zugreift und über einen autorisierten Anwendernamen mit dem entsprechenden Kennwort verfügt, hat Zugriff auf den Host.

Die Sicherheitszertifikate für die Verschlüsselung werden von ESX Server erstellt und auf dem Host gespeichert. Die Zertifikate, die zur Absicherung von VirtualCenter- und VI-Web Access-Sitzungen verwendet werden, wurden nicht von einer vertrauenswürdigen Zertifizierungsinstanz unterzeichnet und bieten daher nicht die Authentifizierungssicherheit, die in einer Produktionsumgebung notwendig sein kann. So sind beispielsweise selbst unterzeichnete Zertifikate gegenüber Man-in-the-Middle-Angriffen empfindlich. Wenn Sie verschlüsselte Fernverbindungen extern verwenden möchten, kann es ggf. sinnvoll sein, ein Zertifikat von einer beglaubigten Zertifizierungsinstanz zu erwerben oder ein eigenes Sicherheitszertifikat für die SSL-Verbindungen zu verwenden.

Der Standardspeicherort für das Zertifikat ist `/etc/vmware/ssl/` auf dem ESX Server-Host. Das Zertifikat besteht aus zwei Dateien: dem Zertifikat selbst (`rui.crt`) und der persönlichen Schlüsseldatei (`rui.key`).

Hinzufügen von Zertifikaten und Änderungen der Web-Proxyeinstellungen des ESX Servers

Beachten Sie beim Hinzufügen von Zertifikaten zu ESX Server und bei der Planung von Verschlüsselung und Anwendersicherheit Folgendes:

- ESX Server kann Kennwortsätze (verschlüsselte Schlüssel) nicht verarbeiten. Wenn Sie eine Kennparole einrichten, können ESX Server-Prozesse nicht richtig aufgerufen werden. Vermeiden Sie daher die Verwendung von Zertifikaten, die dieses Verfahren verwenden.

- Sie können den Web-Proxy so konfigurieren, dass er an einer anderen Stelle als am Standardspeicherort nach Zertifikaten sucht. Dies ist hilfreich, wenn die Zertifikate zentral auf einem Computer gespeichert werden sollen, damit mehrere Hosts die Zertifikate verwenden können.

VORSICHT Wenn Sie Zertifikate an einem anderen Speicherort als dem ESX Server-Host speichern, können Sie auf die Zertifikate nicht zugreifen, wenn die Verbindung des Hosts zu dem Computer mit den Zertifikaten getrennt wird.

- Zur Unterstützung von Verschlüsselung für Anwendernamen, Kennwörter und Pakete wird SSL standardmäßig für VI-Web Access- und Web SDK-Verbindungen aktiviert. Wenn Sie diese Verbindungen in der Form einstellen müssen, dass die Übertragungen nicht verschlüsselt werden, deaktivieren Sie SSL für Ihre VI-Web Access Verbindung oder die Web SDK Verbindung, indem Sie die Verbindung von HTTP auf HTTPS umstellen, wie in „Änderung der Sicherheitseinstellungen für einen Web-Proxy-Dienst“ auf Seite 230 beschrieben. Deaktivieren Sie SSL nur dann, wenn Sie eine vollständig vertrauenswürdige Umgebung für die Clients geschaffen haben, d. h. wenn Firewalls installiert wurden und die Übertragungen zum und vom Host vollständig isoliert sind. Die Deaktivierung von SSL kann die Leistung von VI-Web Access erhöhen, da der für die Verschlüsselung notwendige Overhead vermieden wird.
- Um den Missbrauch von ESX Server-Diensten wie dem internen Web-Server, auf dem VI-Web Access ausgeführt wird, zu verhindern, kann auf die meisten internen ESX Server-Dienste nur über Port 443, den für HTTPS-Übertragungen verwendeten Port, zugegriffen werden. Port 443 dient als Reverse-Proxy für ESX Server. Sie können ein Verzeichnis der Dienste auf ESX Server über die Begrüßungsseite von HTTP sehen, aber Sie können nur direkt auf diese Dienste zugreifen, wenn Sie über die entsprechenden Berechtigungen verfügen. Sie können diese Einstellung ändern, sodass auf bestimmte Dienste direkt über HTTP-Verbindungen zugegriffen werden kann. VMware empfiehlt, dass Sie diese Änderung nur vornehmen, wenn Sie ESX Server in einer vertrauenswürdigen Umgebung verwenden.
- Wenn Sie VirtualCenter und VI-Web Access aktualisieren, wird das Zertifikat beibehalten. Wenn Sie VirtualCenter und VI-Web Access deinstallieren, wird das Verzeichnis, in dem sich das Zertifikat befindet, nicht von der Servicekonsole gelöscht.

Konfiguration des Web-Proxys zur Suche nach Zertifikaten an anderen Speicherorten

1. Melden Sie sich als Root-Anwender auf der Servicekonsole an.
2. Wechseln Sie in das Verzeichnis `/etc/vmware/hostd/`.
3. Öffnen Sie die Datei `config.xml` mit nano oder einem anderen Texteditor und bearbeiten Sie das folgende XML-Segment:

```
<ssl>
   <!-- The server private key file -->
   <privateKey>/etc/vmware/ssl/rui.key</privateKey>
   <!-- The server side certificate file -->
   <certificate>/etc/vmware/ssl/rui.crt</certificate>
</ssl>
```

4 Ersetzen Sie `/etc/vmware/ssl/rui.key` durch das absolute Verzeichnis zu der persönlichen Schlüsseldatei, die Sie von der beglaubigten Zertifikatsbehörde erhalten haben.

   Dieses Verzeichnis kann sich auf dem ESX Server-Host oder auf einem zentralisierten Computer, auf dem die Zertifikate und Schlüssel für Ihr Unternehmen gespeichert sind, befinden.

HINWEIS Belassen Sie die XML-Tags `<privateKey>` und `</privateKey>` an ihrem Platz.

5 Ersetzen Sie `/etc/vmware/ssl/rui.crt` durch das absolute Verzeichnis zu der Zertifikatsdatei, die Sie von der beglaubigten Zertifikatsbehörde erhalten haben.

VORSICHT Löschen Sie die ursprünglichen Dateien `rui.key` und `rui.crt` nicht. Diese Dateien werden vom ESX Server-Host verwendet.

6 Speichern Sie die Änderungen und schließen Sie die Datei.

7 Geben Sie folgenden Befehl ein, um den Prozess `vmware-hostd` neu zu starten:

```
service mgmt-vmware restart
```

Änderung der Sicherheitseinstellungen für einen Web-Proxy-Dienst

1 Melden Sie sich als Root-Anwender auf der Servicekonsole an.

2 Wechseln Sie in das Verzeichnis `/etc/vmware/hostd/`.

3 Öffnen Sie die Datei `config.xml` mit nano oder einem anderen Texteditor und bearbeiten Sie das folgende XML-Segment:

```
<proxysvc>
   <path>/usr/lib/vmware/hostd/libproxysvc.so</path>
   <http>
      <port>80</port>
      <proxyDatabase>
         <server id="0">
            <namespace> / </namespace>
            <host> localhost </host>
            <port> 9080 </port>
         </server>
         <redirect id="0"> /ui </redirect>
```

```
            <redirect id="1"> /mob </redirect>
            <redirect id="2"> /sdk </redirect>
         </proxyDatabase>
      </http>
      <https>
         <port>443</port>
         <proxyDatabase>
            <server id="0">
               <namespace> / </namespace>
               <host> localhost </host>
               <port> 9080 </port>
            </server>
            <server id="1">
               <namespace> /sdk </namespace>
               <host> localhost </host>
               <port> 8085 </port>
            </server>
            <server id="2">
               <namespace> /ui </namespace>
               <host> localhost </host>
               <port> 8080 </port>
            </server>
            <server id="3">
               <namespace>/mob</namespace>
               <host>localhost</host>
               <port>8087</port>
            </server>
         </proxyDatabase>
      /https>
</proxysvc>
```

4 Verschieben Sie für jeden HTTPS-Dienst, auf den Sie über HTTP zugreifen wollen, folgenden Abschnitt aus dem HTTPS-Bereich in den HTTP-Bereich:

```
<server id="ID_Nummer">
   <namespace> Dienstdomäne </namespace>
   <host> localhost </host>
   <port> Port-Nummer </port>
</server>
```

Wobei:

- *ID_Nummer* eine ID-Nummer für das Server-ID-XML-Tag ist. ID-Nummern müssen im HTTP-Bereich eindeutig sein.
- *Dienstdomäne* der Name des Dienstes ist, den Sie verschieben, z. B. `/sdk` oder `/mob`.
- *Port-Nummer* die Nummer des Ports ist, der dem Dienst zugewiesen wurde. Sie können dem Dienst eine andere Port-Nummer zuweisen.

5 Entfernen Sie dann im HTTP-Abschnitt die Umleitungsbefehle (<redirect>) für die Dienste, die Sie verschieben.

6 Speichern Sie die Änderungen und schließen Sie die Datei.

7 Geben Sie folgenden Befehl ein, um den Prozess `vmware-hostd` neu zu starten:

```
service mgmt-vmware restart
```

Gehen Sie genauso vor, wenn Sie einen HTTP-Dienst in den HTTPS-Abschnitt verschieben, fügen Sie dabei jedoch einen Umleitungsbefehl in den HTTP-Bereich ein, wenn Sie den Dienst verschoben haben. Fügen Sie den neuen Umleitungsbefehl nach den anderen Umleitungsbefehlen ein und weisen Sie dem Redirect-Tag eine eindeutige ID-Nummer zu.

Beispiel: Konfiguration von VI-Web Access zur Kommunikation über einen unsicheren Port

VI-Web Access kommuniziert mit einem ESX Server-Host normalerweise über einen sicheren Port (HTTPS, 443). Wenn Sie sich in einer vollständig vertrauenswürdigen Umgebung befinden, können Sie einen unsicheren Port verwenden (zum Beispiel HTTP, 80). Ändern Sie dazu den Bereich Proxy-Dienste in der Datei `/etc/vmware/hostd/config.xml` wie oben beschrieben. Das Ergebnis sieht folgendermaßen aus, wobei die geänderten und verschobenen Bereiche fett hervorgehoben sind. Der Server-Abschnitt für `/ui` (den VI-Web Access-Dienst) wurde in den HTTP-Bereich verschoben und der Umleitungsbefehl für `/ui` wurde entfernt.

```
<proxysvc>
   <path>/usr/lib/vmware/hostd/libproxysvc.so</path>
   <http>
      <port>80</port>
      <proxyDatabase>
         <server id="0">
            <namespace> / </namespace>
            <host> localhost </host>
            <port> 9080 </port>
         </server>
         <server id="1">
            <namespace> /ui </namespace>
            <host> localhost </host>
            <port> 8080 </port>
         </server>
         <redirect id="0"> /mob </redirect>
         <redirect id="1"> /sdk </redirect>
      </proxyDatabase>
   </http>
   <https>
      <port>443</port>
      <proxyDatabase>
```

```
            <server id="0">
               <namespace> / </namespace>
               <host> localhost </host>
               <port> 9080 </port>
            </server>
            <server id="1">
               <namespace> /sdk </namespace>
               <host> localhost </host>
               <port> 8085 </port>
            </server>
            <server id="2">
               <namespace>/mob</namespace>
               <host>localhost</host>
               <port>8087</port>
            </server>
         </proxyDatabase>
      </https>
   </proxysvc>
```

Erneutes Erzeugen von Zertifikaten

Der ESX Server-Host erzeugt Zertifikate, wenn Sie den Host nach der Installation zum ersten Mal starten. Anschließend sucht bei jedem Neustart des `vmware-hostd` Prozesses das `vmware-mgmt` Skript nach vorhandenen Zertifikatsdateien (`rui.crt` und `rui.key`). Für den Fall, dass es keine findet, werden neue Zertifikatsdateien erzeugt.

Unter gewissen Umständen kann es sein, dass Sie den ESX Server-Host dazu zwingen müssen, neue Zertifikate zu erzeugen. Typischerweise müssen Sie nur dann neue Zertifikate erstellen, wenn:

- Sie den Host-Namen ändern.
- Versehentlich Zertifikate löschen.

Um neue Zertifikate für den ESX Server-Host zu erzeugen

1. Wechseln Sie in das Verzeichnis `/etc/vmware/ssl`.
2. Erstellen Sie Backups aller existierenden Zertifikate, indem Sie die folgenden Befehle ausführen:

   ```
   mv rui.crt orig.rui.crt
                 mv rui.key orig.rui.key
   ```

HINWEIS Wenn Sie Zertifikate erstellen, weil Sie versehentlich Zertifikate gelöscht haben, brauchen Sie den Backup-Schritt nicht auszuführen.

3. Geben Sie folgenden Befehl ein, um den Prozess `vmware-hostd` neu zu starten:

   ```
   service mgmt-vmware restart
   ```

4 Bestätigen Sie, dass der ESX Server-Host neue Zertifikate erstellt hat, indem Sie den folgenden Befehl ausführen, der die Zeitstempel der neuen Zertifikatsdateien mit orig.rui.crt und orig.rui.key vergleicht:

```
ls –la
```

Delegierte der virtuellen Maschine für NFS-Speicher

Für die meisten Vorgänge auf virtuellen Maschinen benötigt ein ESX Server Zugriff auf die Dateien der virtuellen Maschine. So muss ESX Server zum Beispiel zum Hoch- oder Herunterfahren von virtuellen Maschinen Dateien auf dem Datenträger, auf dem die Dateien der virtuellen Festplatte gespeichert sind, erstellen, bearbeiten und löschen können.

Wenn Sie virtuelle Maschinen auf einem NFS-Datastore erstellen, konfigurieren oder verwalten, erfolgt dies durch einen besonderen Anwender, den sog. delegierten Anwender. Die Identität des delegierten Anwenders wird von ESX Server für den gesamten Datenverkehr zum und vom darunterliegenden Dateisystem verwendet.

Der delegierte Standardanwender für den ESX Server-Host ist `root`. Nicht alle NFS-Datastores akzeptieren jedoch `Root` als den delegierten Anwender. NFS-Administratoren können Datenträger mit aktiviertem Root Squash exportieren. Die Funktion `root squash` bildet einen Root auf einen Anwender ohne wesentliche Privilegien auf dem NFS-Server ab und beschränkt so die Berechtigungen des Root-Anwenders. Diese Funktion wird meistens verwendet, um unerlaubten Zugriff auf Dateien auf dem NFS-Datenträger zu verhindern. Wenn das NFS-Volume exportiert wurde, während `Root-Squash` aktiviert war, kann es sein, dass der NFS-Server den Zugriff auf den ESX Server-Host verbietet. Um sicherzustellen, dass Sie virtuelle Maschinen über Ihren Host anlegen und verwalten können, muss der NFS-Administrator die `Root-Squash` Funktion deaktivieren oder den physischen Netzwerkadapter des ESX Server-Hosts der Liste der vertrauten Server hinzufügen.

Wenn der NFS-Administrator keine dieser beiden Aktionen durchführen möchte, können Sie den Delegierten durch die experimentellen ESX Server Funktionen auf eine andere Identität setzen. Diese Identität muss derjenigen des Inhabers des Verzeichnisses auf dem NFS-Server entsprechen. Im anderen Fall kann der ESX Server-Host keine Vorgänge auf der Dateiebene durchführen. Um einem Delegierten eine andere Identität anzulegen, benötigen Sie die folgenden Informationen:

- Benutzername des Verzeichnisinhabers
- Benutzer-ID (UID) des Verzeichnisinhabers
- Gruppen-ID (GID) des Verzeichnisinhabers

Dann verwenden Sie diese Informationen, um die Einstellungen des Delegierten für den ESX Server-Host so zu ändern, dass sie mit den Daten des Verzeichnisinhabers übereinstimmen. Damit kann der NFS-Datastore den ESX Server-Host korrekt erkennen. Der Delegierte wird global konfiguriert und dieselbe Identität wird zum Zugriff auf jedes Volume verwendet.

Die Einrichtung des delegierten Anwenders auf einem ESX Server-Host umfasst folgende Schritte:

- Aus der Tabelle Benutzer & Gruppen für einen VI Client, der direkt auf einem ESX Server-Host ausgeführt wird, haben Sie zwei Möglichkeiten:
  - Bearbeiten Sie den Benutzernamen `vimuser`, um die richtige UID und GID einzugeben. Bei `vimuser` handelt es sich um einen Benutzer des ESX Server-Hosts, der dazu eingerichtet wurde, Ihnen die Einrichtung von Delegierten zu vereinfachen. Standardmäßig hat der `vimuser` die UID 12 und die GID 20.
  - Fügen Sie einen völlig neuen Benutzer zum ESX Server-Host dazu. Dazu geben Sie den Delegierten-Benutzernamen, die UID und GID an.

  Sie müssen einen dieser Schritte ausführen und dies unabhängig davon, ob Sie den Host durch eine direkte Verbindung oder VirtualCenter Server verwalten. Des Weiteren müssen Sie sicherstellen, dass der Delegierte (`vimuser` oder der Delegierte, den Sie anlegen) über alle ESX Server Hosts identisch ist, die den NFS-Datastore verwenden. Informationen zum Hinzufügen von Anwendern erhalten Sie unter „Verwaltung der Anwendertabelle“ auf Seite 222.

- Konfigurieren Sie einen Delegierten für virtuelle Maschinen als Teil des Sicherheitsprofils für den Host hinzu (s. u.).

  Konfigurieren Sie das Sicherheitsprofil über VirtualCenter oder einen VI Client, der direkt auf dem ESX Server-Host ausgeführt wird. Diese Aufgabe wird sinnvoller über VirtualCenter ausgeführt, da Sie in einer Session jeden Host nacheinander bearbeiten können. In diesem Fall handelt es sich bei den Benutzern, die Zugriff auf die NFS-Volumes haben, um diejenigen, die in der Windows-Domäne vertreten sind.

WARNHINWEIS Die Änderung des Delegierten für einen ESX Server-Host ist als experimentell zu verstehen, demzufolge unterstützt VMware diese Form der Implementierung derzeit nicht. Die Verwendung dieser Funktion kann zu einem unerwarteten Verhalten führen.

Änderung des delegierten Anwenders für virtuelle Maschinen

1 Melden Sie sich über den ESX Server-Host im VI Client an.

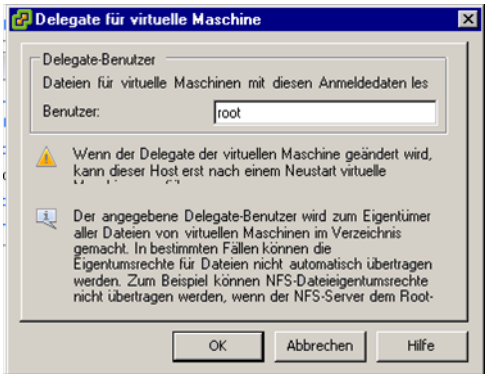
2 Wählen Sie den Server aus dem Inventar aus.

  Die Hardware-Konfiguration für diesen Server wird mit der Registerkarte „Übersicht“ angezeigt.

3 Klicken Sie auf **Wartungsmodus einschalten**.

4 Klicken Sie auf die Registerkarte und dann auf **Sicherheitsprofil**.

5 Klicken Sie auf **Delegierte Anwender für virtuelle Maschinen** > **Bearbeiten**. Das Dialogfeld **Delegierte Anwender für virtuelle Maschinen** wird angezeigt.


Delegate für virtuelle Maschine
Delegate-Benutzer
Dateien für virtuelle Maschinen mit diesen Anmeldedaten les
Benutzer:
root
Wenn der Delegate der virtuellen Maschine geändert wird, kann dieser Host erst nach einem Neustart virtuelle
Der angegebene Delegate-Benutzer wird zum Eigentümer aller Dateien von virtuellen Maschinen im Verzeichnis gemacht. In bestimmten Fällen können die Eigentumsrechte für Dateien nicht automatisch übertragen werden. Zum Beispiel können NFS-Dateieigentumsrechte nicht übertragen werden, wenn der NFS-Server dem Root-
OK
Abbrechen
Hilfe

6 Geben Sie den Anwendernamen des delegierten Anwenders ein.

7 Klicken Sie auf **OK**.

8 Starten Sie den ESX Server-Host neu.

Nach dem Neustart des Hosts wird die Einstellung des delegierten Anwenders sowohl in VirtualCenter als auch im direkt auf dem ESX Server-Host ausgeführten VI Client angezeigt.

Sicherheit der Servicekonsole 12

Dieses Kapitel enthält grundlegende Sicherheitsempfehlungen für die Servicekonsole und erläutert einige der in die Servicekonsole integrierten Sicherheitsfunktionen. Die Servicekonsole ist eine Management-Schnittstelle für ESX Server, daher ist ihre Sicherheit sehr wichtig. Um die Servicekonsole gegen unbefugten Zugriff und Missbrauch zu schützen, beschränkt VMware bestimmte Parameter, Einstellungen und Aktivitäten der Servicekonsole.

Diese Beschränkungen wurden dazu entworfen, die Sicherheit für ESX Server zu erhöhen. Sie können diese Beschränkungen lockern, um Ihre spezifischen Konfigurationsbedürfnisse zu erfüllen. In diesem Fall müssen Sie aber tatsächlich in einer vertrauenswürdigen Umgebung arbeiten und genug andere Sicherheitsmaßnahmen ergriffen haben, um das Netzwerk als Ganzes und die an den ESX Server-Host angeschlossenen Geräte zu schützen.

In diesem Kapitel werden folgende Themen behandelt:

- „Allgemeine Sicherheitsempfehlungen“ auf Seite 238
- „Konfiguration der Servicekonsolen-Firewall“ auf Seite 240
- „Kennwortbeschränkungen“ auf Seite 244
- „Schlüsselqualität“ auf Seite 252
- „Setuid- und setgid-Anwendungen“ auf Seite 252
- „SSH-Sicherheit“ auf Seite 255
- „Sicherheitspatches und Sicherheitslücken-Scanner“ auf Seite 257

Allgemeine Sicherheitsempfehlungen

Beachten Sie bei der Überprüfung der Servicekonsolensicherheit und der Verwaltung der Servicekonsole folgende Sicherheitsempfehlungen:

- **Installation von Antiviren-Software.**

  Auch wenn Sie einen ESX Server-Host betreiben können, ohne dass die Servicekonsole an ein Netzwerk angeschlossen ist, ermöglichen die meisten Implementierungen der Servicekonsole den Netzwerkzugriff. Da die Servicekonsole ein vollständiges Betriebssystem ist, sollten Sie es - wie jedes Betriebssystem und jede virtuelle Maschine am Standort - vor Viren schützen. Wenn Sie in Ihrem Unternehmen bereits Antivirenprogramme für Linux verwenden, können Sie diese auch auf der Servicekonsole verwenden. Sie können Einbruchs- und Rootkit-Erkennungs-programme von Drittanbietern wie z. B. Tripwire installieren.

HINWEIS Antiviren-Software kann die Leistung beeinflussen. Wenn Sie sich sicher sind, dass sich der ESX Server-Host in einer vollständig vertrauenswürdigen Umgebung befindet, können Sie diese Sicherheitsmaßnahme gegen Leistungsnachteile abwägen.

- **Beschränkung des Anwenderzugriffs.**

  Beschränken Sie zur Verbesserung der Sicherheit den Anwenderzugriff auf die Servicekonsole und setzen Sie Policys für die Zugriffssicherheit wie z. B. Kennwortbeschränkungen um – zum Beispiel Vorgabe der Kennwortlänge, Zeitbeschränkungen für Kennwörter und Verwendung eines `grub`-Kennworts beim Hochfahren des Hosts.

  Die Servicekonsole hat privilegierten Zugriff auf bestimmte Teile von ESX Server. Daher sollten nur vertrauenswürdige Anwender Zugriff darauf erhalten. In der Standardeinstellung ist der Root-Zugriff beschränkt, wodurch eine SSH-Anmeldung als Root nicht möglich ist. Wir empfehlen, diese Standardeinstellung beizubehalten. Systemadministratoren für ESX Server sollten sich als normale Anwender anmelden und dann `sudo` verwenden, um bestimmte Aufgaben, die Root-Privilegien erfordern, auszuführen.

  Versuchen Sie auch, so wenige Prozesse wie möglich auf der Servicekonsole auszuführen. Im Idealfall sollten nur die Prozesse, Dienste und Agenten ausgeführt werden, die wirklich notwendig sind, wie zum Beispiel Antivirenprogramme, Backups für die virtuellen Maschinen usw.

- **Verwaltung der ESX Server-Hosts über den VI Client.**

  Verwenden Sie den VI Client, VI-Web Access oder ein Netzwerk-Management-Programm von Drittanbietern zur Verwaltung der ESX Server-Hosts, wenn dies möglich ist, statt als Root über die Befehlszeilenoberfläche zu agieren. Mit dem VI Client können Sie die Anzahl der Konten, die Zugriff auf die Servicekonsole

haben, einschränken, Verantwortungen sicher weitergeben und Rollen einrichten, damit Administratoren und Anwender keine Funktionen nutzen können, die sie nicht benötigen.

- **Ausschließliche Verwendung von VMware Quellen für Aktualisierungen von ESX Server-Komponenten auf der Servicekonsole.**

  Auf der Servicekonsole werden zur Unterstützung von notwendigen Management-Schnittstellen oder -Aufgaben viele Pakete von Drittanbietern wie zum Beispiel der Tomcat Web-Dienst ausgeführt. Bei VMware können diese Pakete nur über eine VMware Quelle aktualisiert werden. Wenn Sie einen Download oder Patch aus einer anderen Quelle verwenden, können die Sicherheit und die Funktionen der Servicekonsole gefährdet werden. Überprüfen Sie die Internetseiten von Drittanbietern und die VMware Wissensbasis regelmäßig auf Sicherheitswarnungen.

Anmelden an der Servicekonsole

Obwohl die meisten Konfigurationsvorgänge für ESX Server über den VI Client ausgeführt werden, müssen bestimmte Sicherheitsfunktionen über die Befehlszeilenoberfläche der Servicekonsole konfiguriert werden. Zur Verwendung der Befehlszeilenoberfläche müssen Sie sich auf dem Host anmelden. Wenn Sie direkten Zugriff auf den ESX Server-Host haben, können Sie sich auf der physischen Konsole auf diesem Computer anmelden. Drücken Sie dazu auf dem Anmeldebildschirm Alt-F2. Verwenden Sie bei Fernverbindungen SSH oder eine andere Fernsteuerungsverbindung, um eine Sitzung auf dem Host aufzurufen.

In beiden Fällen – sowohl bei der lokalen Anmeldung als auch bei der Anmeldung über eine Fernverbindung wie SSH – müssen Sie sich mit einem Anwendernamen und einem Kennwort anmelden, dass der ESX Server-Host erkennt. Weitere Informationen zu Anwendernamen und Kennwörtern für ESX Server-Hosts finden Sie unter „Verwaltung von Anwendern und Gruppen auf ESX Server-Hosts“ auf Seite 219.

Wenn Sie sich auf dem Host anmelden, um Vorgänge auszuführen, für die Root- Privilegien notwendig sind, sollten Sie sich zuerst als normaler Anwender auf der Servicekonsole anmelden und dann über den Befehl `su` oder den zu bevorzugenden Befehl `sudo` als Root anmelden. Der Befehl `sudo` erhöht die Sicherheit, da er nur für bestimmte, ausgewählte Vorgänge Root-Privilegien gewährt, während `su` Root-Privilegien für alle Vorgänge gewährt. Durch `sudo` sind außerdem alle Vorgänge besser nachvollziehbar, da alle `sudo` Vorgänge protokolliert werden, wohingegen bei `su`, der ESX Server nur protokolliert wird, dass der Anwender durch `su` auf Root umgeschaltet hat.

Zusätzlich zu den ESX-spezifischen Befehlen können Sie über die Befehlszeilenoberfläche der Servicekonsole auch viele Linux- und Unix-Befehle ausführen. Detaillierte Benutzungshinweise zu Servicekonsolenbefehlen erhalten Sie über den Befehl `man <command_name>`, mit dem Sie die Hilfeseiten aufrufen.

Konfiguration der Servicekonsolen-Firewall

ESX Server enthält eine Firewall zwischen der Servicekonsole und dem Netzwerk. Damit die Integrität der Servicekonsole sichergestellt wird, hat VMware die Anzahl der standardmäßig freigegebenen Firewall-Ports reduziert. Bei der Installation wird die Firewall der Servicekonsole so konfiguriert, dass der gesamte eingehende und ausgehende Datenverkehr auf allen Ports außer auf 902, 80, 443 und 22 blockiert wird. Die genannten Ports werden für die grundlegende Kommunikation mit ESX Server verwendet. Durch diese Einstellung ist die Sicherheit für den ESX Server-Host sehr hoch.

HINWEIS Die Firewall lässt auch Internet Control Message Protocol (ICMP)-Pings und Kommunikation mit DHCP- und DNS- Clients (nur UDP) zu.

In vertrauenswürdigen Umgebungen kann eine niedrigere Sicherheitsstufe möglich sein. In diesem Fall können Sie die Firewall entweder auf mittlere oder niedrige Sicherheit setzen:

- **Mittlere Sicherheit** – Der gesamte eingehende Datenverkehr wird blockiert, ausgenommen ist Datenverkehr auf den Standard-Ports (902, 433, 80 und 22) sowie auf allen Ports, die Sie freigeben. Ausgehender Datenverkehr wird nicht blockiert.
- **Niedrige Sicherheit** – Weder eingehender noch ausgehender Datenverkehr wird blockiert. Diese Einstellung entspricht der Deaktivierung der Firewall.

Da die standardmäßig freigegebenen Ports stark beschränkt sind, müssen Sie ggf. nach der Installation zusätzliche Ports freigeben. Ein Verzeichnis der häufig verwendeten Ports, die Sie ggf. freigeben müssen, finden Sie unter „TCP- und UDP-Ports für den Management-Zugriff“ auf Seite 187.

Beachten Sie, dass Sie durch das Hinzufügen von unterstützten Diensten und Management-Agenten, die zum effektiven Betrieb von ESX Server notwendig sind, weitere Ports in der Firewall der Servicekonsole freigeben. Dienste und Management-Agenten werden über VirtualCenter hinzugefügt. Weitere Informationen hierzu finden Sie unter „Freigeben von Firewall-Ports für unterstützte Dienste und Management-Agenten“ auf Seite 192.

Neben den Ports, die für diese Dienste und Agenten freigegeben werden, müssen Sie eventuell andere Ports freigeben, wenn Sie bestimmte Geräte, Dienste oder Agenten wie z. B. Speichergeräte, Backup-Agenten oder Management-Agenten konfigurieren. Wenn Sie zum Beispiel Veritas NetBackup™ 4.5 als Backup-Agenten verwenden, müssen Sie die Ports 13720, 13724, 13782 und 13783 freigeben, die NetBackup für Client-Medien-Übertragungen, Datenbank-Backups, Anwender-Backups oder Wiederherstellungen usw. verwendet. Informationen zu den für bestimmte Anwendungen freizugebenden Ports finden Sie in den Herstellerspezifikationen für das Gerät, den Dienst oder den Agenten.

Im Weiteren wird erläutert, wie die Sicherheitsstufe der Servicekonsole geändert werden kann und wie man Ports für zusätzliche Geräte, Dienste und Agenten freigibt.

HINWEIS Jedes Mal, wenn Sie die Sicherheitseinstellung senken oder zusätzliche Ports öffnen, erhöhen Sie das Risiko eines Einbruchs in Ihr Netzwerk. Wägen Sie genau ab, wie wichtig Ihnen Zugriffsrechte im Kontrast zur Sicherheit des Netzwerkes sind.

Änderung der Sicherheitsstufe der Servicekonsole

Die Änderung der Sicherheitsstufe für die Servicekonsole besteht aus zwei Teilen: Bestimmung des Sicherheitsniveaus der Servicekonsolen-Firewall und Zurücksetzen der Einstellungen der Servicekonsolen-Firewall. Um überflüssige Schritte zu vermeiden, überprüfen Sie immer die Firewalleinstellungen, bevor Sie sie ändern.

Bestimmung der Sicherheitsstufe der Servicekonsolen-Firewall

1 Melden Sie sich auf der Servicekonsole an und erlangen Sie Root-Privilegien.

2 Führen Sie folgende zwei Befehle aus, um zu bestimmen, ob eingehender und ausgehender Datenverkehr erlaubt oder blockiert wird:

```
esxcfg-firewall -q incoming
esxcfg-firewall -q outgoing
```

3 Die Ergebnisse bedeuten Folgendes:

Befehlszeilenausgabe	Sicherheitsstufe
`Incoming ports blocked by default.` `Outgoing ports blocked by default.`	Hoch
`Incoming ports blocked by default.` `Outgoing ports not blocked by default.`	Mittel
`Incoming ports not blocked by default.` `Outgoing ports not blocked by default.`	Niedrig

Festlegung der Sicherheitsstufe der Servicekonsolen-Firewall

1 Melden Sie sich auf der Servicekonsole an und erlangen Sie Root-Privilegien.

2 Führen Sie je nach Bedarf einen der folgenden Befehle aus.

- Festlegung der mittleren Sicherheitsstufe für die Servicekonsolen-Firewall:

  ```
  esxcfg-firewall --allowOutgoing --blockIncoming
  ```

- Festlegung der niedrigen Sicherheitsstufe für die virtuelle Firewall:

  ```
  esxcfg-firewall --allowIncoming --allowOutgoing
  ```

VORSICHT Der oben stehende Befehl deaktiviert den Schutz durch die Firewall vollständig.

- Festlegung der hohen Sicherheitsstufe für die Servicekonsolen-Firewall:

  ```
  esxcfg-firewall --blockIncoming --blockOutgoing
  ```

3 Geben Sie folgenden Befehl ein, um den Prozess `vmware-hostd` neu zu starten:

```
service mgmt-vmware restart
```

Die Änderung der Sicherheitsstufe der Servicekonsolen-Firewall beeinflusst bestehende Verbindungen nicht. Wenn die Firewall zum Beispiel auf niedriger Sicherheitsstufe ausgeführt wird und ein Backup auf einem Port ausgeführt wird, den Sie nicht ausdrücklich freigegeben haben, beendet eine Erhöhung der Sicherheitsstufe auf „Hoch“ das Backup nicht. Weil die Firewall so konfiguriert ist, dass die Pakete für zuvor hergestellte Verbindungen durchgelassen werden, wird das Backup abgeschlossen und die neue Verbindung freigegeben. Anschließend werden für diesen Port keine weiteren Verbindungen akzeptiert.

Freigeben und Blockieren von Ports in der Servicekonsolen-Firewall

Wenn Sie Geräte, Dienste oder Agenten von Drittanbietern installieren, können Sie Ports in der Servicekonsolen-Firewall freigeben. Bevor Sie Ports für das Gerät oder den Dienst freigeben, konsultieren Sie die Herstellerspezifikationen, um zu bestimmen, welche Ports freigegeben werden müssen.

Wenn Sie einen Port blockieren, werden aktive Sitzungen des Dienstes, der den Port verwendet, nicht automatisch getrennt, wenn Sie den Port blockieren. Wenn Sie zum Beispiel ein Backup durchführen und Sie den Port für den Backup-Agenten schließen, wird das Backup fortgesetzt, bis es vollständig ist und der Agent die Verbindung freigibt.

Verwenden Sie die folgenden Vorgänge nur, wenn Sie Ports für Dienste oder Agenten freigeben oder blockieren, die nicht über den VI Client konfiguriert werden können. Informationen zur Konfiguration zusätzlicher Ports in VirtualCenter finden Sie unter „Freigeben von Firewall-Ports für unterstützte Dienste und Management-Agenten“ auf Seite 192.

WARNHINWEIS VMware Support unterstützt das Öffnen und Blockieren der Firewall-Ports nur durch den VI Client oder den `esxcfg-firewall` Befehl, wie im Folgenden beschrieben. Eine Verwendung anderer Methoden oder Skripte zum Öffnen oder Blockieren der Firewall-Ports kann zu einem unerwarteten Verhalten führen.

Freigabe eines bestimmten Ports in der Servicekonsolen-Firewall

1 Melden Sie sich auf der Servicekonsole an und erlangen Sie Root-Privilegien.

2 Geben Sie folgenden Befehl ein:

```
esxcfg-firewall --openPort <Portnummer>,tcp|udp,in|out,<Portname>
```

Wobei:

- `Port-Nummer` die vom Hersteller angegebene Port-Nummer ist.
- `tcp|udp` das Protokoll ist. Geben Sie `tcp` für TCP-Datenverkehr oder `udp` für UDP-Datenverkehr an.
- `in|out` ist die Richtung des Datenverkehrs. Geben Sie `in` an, um einen Port für eingehenden Datenverkehr freizugeben, oder `out`, um den Port für ausgehenden Datenverkehr zu öffnen.
- `Port-Name` ist ein beschreibender Name. Der Name muss nicht eindeutig sein, sollte jedoch Sinn ergeben, damit der Dienst oder Agent identifiziert werden kann, der den Port verwendet.

Beispiel:

```
esxcfg-firewall --openPort 6380,tcp,in,Navisphere
```

3 Geben Sie folgenden Befehl ein, um den Prozess `vmware-hostd` neu zu starten:

```
service mgmt-vmware restart
```

Blockierung eines bestimmten Ports in der Servicekonsolen-Firewall

1 Melden Sie sich auf der Servicekonsole an und erlangen Sie Root-Privilegien.

2 Geben Sie folgenden Befehl ein:

```
esxcfg-firewall --closePort <Portnummer>,tcp|udp,in|out,<Portname>
```

Für den Befehl `-closePort` ist das Argument `Port-Name` optional.

Beispiel:

```
esxcfg-firewall --closePort 6380,tcp,in
```

3 Geben Sie folgenden Befehl ein, um den Prozess `vmware-hostd` neu zu starten:

```
service mgmt-vmware restart
```

Sie können die Option `-closepPort` verwenden, um nur die Ports zu blockieren, die Sie mit der Option `-openPort` freigegeben hatten. Wenn Sie ein anderes Verfahren verwendet haben, um den Port freizugeben, müssen Sie auch das entsprechende Gegenstück zu dem Verfahren verwenden, um ihn zu blockieren. So können Sie zum Beispiel den SSH-Port (22) nur blockieren, indem Sie die eingehende und ausgehende SSH-Server-Verbindung im VI Client deaktivieren. Weitere Informationen zur Freigabe und zur Blockierung von Ports über den VI Client finden Sie unter „Freigeben von Firewall-Ports für unterstützte Dienste und Management-Agenten“ auf Seite 192.

Kennwortbeschränkungen

Wie leicht sich ein Angreifer auf einem ESX Server-Host anmelden kann, hängt davon ab, wie einfach er eine gültige Anwendername/Kennwort-Kombination finden kann. Ein böswilliger Anwender kann ein Kennwort auf verschiedene Arten erlangen. Zum Beispiel kann er unsicheren Netzwerkdatenverkehr wie z. B. Telnet- oder FTP-Über tragungen auf erfolgreiche Anmeldeversuche abhören.

Ein anderes häufig verwendetes Verfahren zum Knacken eines Kennwortes ist die Verwendung eines Kennwortgenerators. Kennwortgeneratoren können für verschiedene Kennwortangriffe verwendet werden, wie z. B. Brute-Force-Angriffe, bei denen der Generator alle möglichen Zeichenkombinationen bis zu einer bestimmten Kennwortlänge ausprobiert, und Wörterbuchangriffe, bei denen der Generator existierende Wörter und einfache Abwandlungen existierender Wörter ausprobiert.

Der Einsatz von Beschränkungen bezüglich der Länge, der verwendeten Zeichen und der Verwendungsdauer eines Kennwortes kann Angriffe durch Kennwortgeneratoren schwieriger gestalten. Je länger und komplexer ein Kennwort ist, desto schwieriger ist es für einen Angreifer, das Kennwort herauszufinden. Je öfter Anwender ihre Kennwörter ändern müssen, desto schwieriger ist es, ein Kennwort zu finden, das mehrmals funktioniert.

HINWEIS Denken Sie immer an mögliche menschliche Fehler, wenn Sie die Kennwort-Einschränkungen umsetzen. Wenn Sie Kennwörter setzen, die man sich kaum merken kann oder häufige Kennwortänderungen vorschreiben, kann es sein, dass die Benutzer ihre Kennwörter aufschreiben müssen und dadurch deren Sinn verwässern.

Zum Schutz der Kennwortdatenbank gegen Missbrauch wurde Kennwort-Shadowing für ESX Server aktiviert, sodass die Kennwort-Hashs zugriffsgeschützt sind. Außerdem verwendet ESX Server MD5-Kennwort-Hashs, die eine höhere Kennwortsicherheit bieten und es ermöglichen, Kennwörter mit einer Mindestlänge von mehr als 8 Zeichen zu fordern.

ESX Server bietet Kennwortkontrolle auf zwei Ebenen, um Kennwort-Policys für Anwender durchzusetzen und das Risiko des Knackens von Kennwörtern zu begrenzen:

- **Kennwort-Verwendungsdauer** – bestimmt, wie lange ein Anwenderkennwort aktiv sein kann, bevor der Anwender es ändern muss. Dadurch wird sichergestellt, dass das Kennwort oft genug geändert wird, sodass ein Angreifer, der ein Kennwort durch Abhören oder soziale Kontakte erhalten hat, nicht auf ewig auf ESX Server zugreifen kann.
- **Kennwort-Komplexität** – stellt sicher, dass Anwender Kennwörter auswählen, die für Kennwortgeneratoren schwer zu bestimmen sind.

Kennwort-Verwendungsdauer

Damit Kennwörter für die Anwenderanmeldung nicht für lange Zeiträume aktiv bleiben, werden standardmäßig folgende Beschränkungen für die Verwendungsdauer von ESX Server auferlegt:

- **Höchstanzahl von Tagen** – Die Anzahl von Tagen, die ein Anwender ein Kennwort verwenden kann, bevor es geändert werden muss. Die Standardeinstellung für ESX Server ist 90 Tage. Das `Root`-Konto und andere Dienstkonten sind von dieser Einstellung standardmäßig ausgenommen.
- **Mindestanzahl von Tagen** – Die Mindestanzahl von Tagen, die zwischen zwei Kennwortänderungen verstreichen muss. Die Standardeinstellung lautet 0, d. h. die Anwender können ihre Kennwörter jederzeit ändern.
- **Warnhinweiszeit** – ESX Server gibt so viele Tage vor Ablauf des Kennwortes einen Hinweis zur Kennwortänderung aus. Die Standardeinstellung ist 7 Tage. Es werden bei direkten Anmeldungen an der Servicekonsole oder bei einer Verwendung von SSH stets Warnhinweise angezeigt.

Sie können diese Einstellungen mit den Befehlsoptionen von `esxcfg-auth` verschärfen oder lockern. Verwenden Sie den Befehl `chage`, wenn die Verwendungsdauer für einen einzelnen Anwender geändert werden soll.

Änderung der Kennwort-Standardverwendungsdauer für ESX Server

1. Melden Sie sich auf der Servicekonsole an und erlangen Sie Root-Privilegien.
2. Führen Sie nach Bedarf einen oder mehrere der folgenden Befehle aus.
   - Änderung der Höchstanzahl von Tagen, die ein Anwender sein Kennwort behalten kann:

     ```
     esxcfg-auth --passmaxdays=<Anzahl_von_Tagen>
     ```

     wobei `<Anzahl_von_Tagen>` die Höchstanzahl von Tagen vor Ablauf des Kennworts ist.
   - Änderung der Mindestanzahl von Tagen zwischen zwei Kennwortänderungen:

     ```
     esxcfg-auth --passmindays=<Anzahl_von_Tagen>
     ```

     wobei `<Anzahl_von_Tagen>` die Mindestanzahl von Tagen zwischen zwei Kennwortänderungen ist.
   - Änderung der Hinweiszeit vor einer Kennwortänderung:

     ```
     esxcfg-auth --passwarnage=<Anzahl_von_Tagen>
     ```

     wobei `<Anzahl_von_Tagen>` die Anzahl der Tage ist, die ein Anwender vor dem Auslaufen eines Kennwortes Warnhinweise erhält.

Aufhebung der Kennwort-Standardverwendungsdauer für einzelne Anwender oder Gruppen

1 Melden Sie sich auf der Servicekonsole an und erlangen Sie Root-Privilegien.

2 Führen Sie nach Bedarf einen oder mehrere der folgenden Befehle aus.

- Angabe eines neuen Wertes für die Höchstanzahl von Tagen:

  ```
  chage –M <Anzahl_von_Tagen> <Benutzername>
  ```

- Angabe eines neuen Wertes für die Mindestanzahl von Tagen:

  ```
  chage –m <Anzahl_von_Tagen> <Benutzername>
  ```

- Angabe eines neuen Wertes für die Warnhinweiszeit:

  ```
  chage –W <Anzahl_von_Tagen> <Benutzername>
  ```

  Weitere Informationen zu diesen und anderen Optionen des `chage`-Befehls erhalten Sie mit dem Befehl `man chage`.

Kennwort-Komplexität

Standardmäßig verwendet ESX Server das Plug-In `pam_cracklib.so` zur Festlegung der Regeln, die Anwender bei der Erstellung von Kennwörtern beachten müssen, und zur Überprüfung der Kennwortqualität im Erstellungsprozess.

Das Plug-In `pam_cracklib.so` ermöglicht es Ihnen, Standards festzulegen, die alle Kennwörter erfüllen müssen. In der Standardeinstellung wendet ESX Server keine Beschränkungen auf das Root-Kennwort an. Wenn jedoch andere Anwender als der Root-Anwender versuchen, ihr Kennwort zu ändern, müssen die Kennwörter, die sie auswählen, die Standards von `pam_cracklib.so` erfüllen. Außerdem können Anwender (Root-Anwender ausgenommen) nur eine bestimmte Anzahl von Kennwortänderungsversuchen vornehmen, bevor `pam_cracklib.so` eine Warnmeldung ausgibt und schließlich das Dialogfeld zur Änderung des Kennworts schließt. Es gibt bei ESX Server folgende Kennwortstandards und Versuchsbeschränkungen für `pam_cracklib.so`:

- **Mindestlänge** – Der Mindestlänge-Parameter von `pam_cracklib.so` für ESX Server-System wurde auf 9 festgelegt. Das bedeutet, dass der Anwender mindestens 8 Zeichen eingeben muss, wenn er nur eine Zeichenklasse (Kleinbuchstaben, Großbuchstaben, Zahlen usw.) verwendet.

  Der Algorithmus für die Kennwortlänge lässt kürzere Kennwörter zu, wenn der Anwender eine Mischung verschiedener Zeichenklassen zulässt. Zur Berechnung der tatsächlichen Zeichenlänge, die ein Anwender eingeben muss, um ein gültiges Kennwort für eine bestimmte Mindestlängeneinstellung zu erhalten, gilt folgender Kennwortlängen-Algorithmus:

  M – CC = E

Wobei:

- M der Mindestlängenparameter ist.
- CC die Anzahl der Zeichenklassen ist, die der Anwender für das Kennwort verwendet.
- E die Anzahl der Zeichen ist, die der Anwender eingeben muss.

Tabelle 12-1 zeigt, wie der Algorithmus funktioniert, wenn ein Anwender mindestens einen Kleinbuchstaben als Teil des Kennwortes eingibt.

Tabelle 12-1. Ergebnisse des Kennwort-Komplexitätsalgorithmus

Anzahl der Zeichen für ein gültiges Kennwort	Zeichenklassen im Kennwortversuch			
	Kleinbuchstaben	Großbuchstaben	Zahlen	Andere Zeichen
8	Ja			
7	Ja	Ja		
	Ja		Ja	
	Ja			Ja
6	Ja	Ja	Ja	
	Ja	Ja		Ja
	Ja		Ja	Ja
5 [a]	Ja	Ja	Ja	Ja

[a] Das Plug-In `pam_cracklib.so` lässt keine Kennwörter mit weniger als sechs Zeichen zu. Daher ist zwar die mathematisch korrekte Anforderung für ein Kennwort mit vier verschiedenen Zeichenklassen fünf Zeichen, die tatsächliche Anforderung ist jedoch sechs Zeichen.

- **Wiederholungsversuche** – Der Wiederholungsversuchsparameter von `pam_cracklib.so` ist für ESX Server-Systeme auf 3 gesetzt, d. h. dass das Kennwortänderungsdialogfeld nach drei Versuchen, ein gültiges Kennwort einzugeben, von `pam_cracklib.so` geschlossen wird. Der Anwender muss eine neue Sitzung zur Änderung des Kennwortes öffnen, um es erneut zu versuchen.

`pam_cracklib.so` überprüft alle Kennwortänderungsversuche, damit das Kennwort folgende Qualitätskriterien erfüllt:

- Das neue Kennwort darf kein Palindrom sein – d. h. ein Kennwort, das von hinten nach vorn und von vorn nach hinten gelesen werden kann, wie z. B. Radar oder Anna.
- Das neue Kennwort darf keine Umkehrung des alten Kennwortes sein.
- Das neue Kennwort darf keine Buchstabenverdrehung sein – d. h. eine Version des alten Kennwortes, in dem einer oder mehrere Buchstaben nach vorn oder hinten in der Zeichenkette verschoben wurden.

- Das neue Kennwort muss sich vom alten Kennwort durch mehr als nur durch Groß- und Kleinschreibung unterscheiden.
- Das neue Kennwort muss sich vom alten Kennwort durch mehr als nur durch einige Zeichen unterscheiden.
- Das neue Kennwort darf nicht in der Vergangenheit verwendet worden sein. `pam_cracklib.so` verwendet dieses Kriterium nur, wenn Sie eine Regel zur Wiederverwendung von Kennwörtern definiert haben.

  In der Standardeinstellung verwendet ESX Server keine Regeln zur Wiederverwendung von Kennwörtern, sodass `pam_cracklib.so` normalerweise eine Kennwortänderung nicht aus diesem Grund ablehnt. Sie können jedoch eine solche Regel konfigurieren, damit Anwender nicht nur einige wenige Kennwörter abwechselnd verwenden.

  Wenn Sie eine Regel zur Wiederverwendung von Kennwörtern konfigurieren, werden die alten Kennwörter in einer Datei gespeichert, die `pam_cracklib.so` bei jedem Kennwortänderungsversuch abfragt. Die Anzahl der alten Kennwörter, die ESX Server speichert, wird in der Regel festgelegt. Wenn ein Anwender genügend Kennwörter erstellt hat und somit der in der Regel festgelegte Wert erreicht wird, werden die alten Kennwörter aus der Datei anhand ihres Alters gelöscht. Informationen zur Konfiguration der Regel zur Wiederverwendung von Kennwörtern finden Sie unter „Konfiguration einer Regel zur Wiederverwendung von Kennwörtern“ auf Seite 249.
- Das neue Kennwort muss lang und komplex genug sein. Die Anforderungen werden durch Änderung des Komplexitätsparameter von `pam_cracklib.so` mit dem Befehl `esxcfg-auth` konfiguriert. Dieser Befehl ermöglicht Ihnen die Festlegung der Wiederholungsversuche, der Mindestkennwortlänge und verschiedener Zeichenboni. Zeichenboni ermöglichen es den Anwendern, kürzere Kennwörter einzugeben, wenn sich mehrere Zeichenarten in einem Kennwort befinden. Weitere Informationen zur Konfiguration der Kennwortlänge und der Komplexität finden Sie unter „Änderung der Standardkomplexität von Kennwörtern für das Plug-In pam_cracklib.so“ auf Seite 249.

Weitere Informationen zum `pam_cracklib.so`-Plug-In finden Sie in der Linux-Dokumentation.

HINWEIS Das `pam_cracklib.so`-Plug-In, das unter Linux verwendet wird, verfügt über mehr Parameter als das Plug-In für ESX Server. Diese zusätzlichen Parameter können nicht mit `esxcfg-auth` eingerichtet werden.

Konfiguration einer Regel zur Wiederverwendung von Kennwörtern

1 Melden Sie sich auf der Servicekonsole an und erlangen Sie Root-Privilegien.

2 Wechseln Sie in der Eingabeaufforderung über den Befehl `cd /etc/pam.d/` das Verzeichnis.

3 Öffnen Sie mit nano oder einem anderen Texteditor die Datei `system-auth`.

4 Gehen Sie zu der Zeile, die mit folgendem Argument beginnt:

```
password    sufficient    /lib/security/$ISA/pam_unix.so
```

5 Fügen Sie am Ende der Zeile folgende Parameter ein:

```
remember=X
```

Hierbei ist X die Anzahl der alten Kennwörter, die ESX Server für jeden Anwender speichern soll. Trennen Sie den vorhergehenden Parameter und `remember=X` durch ein Leerzeichen.

6 Speichern Sie die Änderungen und schließen Sie die Datei.

7 Wechseln Sie in das Verzeichnis `/etc/security/` und geben Sie folgenden Befehl ein, um eine Nulllängendatei mit dem Namen `opasswd` zu erstellen:

```
touch opasswd
```

8 Geben Sie folgende Befehle ein:

```
chmod 0600 opasswd
               chown root:root /etc/security/opasswd
```

Änderung der Standardkomplexität von Kennwörtern für das Plug-In pam_cracklib.so

1 Melden Sie sich auf der Servicekonsole an und erlangen Sie Root-Privilegien.

2 Geben Sie den folgenden Befehl ein:

```
esxcfg-auth --usecrack=<Versuche> <Mindestlänge> <KB_Bonus> <GB_Bonus>
               <Z_Bonus> <AZ_Bonus>
```

Wobei:

- `Versuche` die Anzahl der Wiederholungsversuche ist, die der Anwender hat, bis ESX Server ihn aus dem Kennwortänderungsmodus ausschließt.
- `Mindestlänge` ist die Mindestanzahl von Zeichen, die ein Anwender eingeben muss, damit das Kennwort angenommen wird. Diese Anzahl ist die Gesamtlänge vor der Anwendung jeglicher Zeichenboni.

Es wird immer mindestens ein Zeichenbonus angewendet, daher ist die Kennwortlänge effektiv ein Zeichen kürzer als im Parameter `Mindestlänge` angegeben. Da `pam_cracklib.so` nur Kennwörter mit mindestens 6 Zeichen annimmt, muss der `Mindestlänge`-Parameter so berechnet werden, dass die Kennwortlänge nach Abzug der Zeichenboni nicht kleiner als 6 sein kann.

- `KB_Bonus` ist die Anzahl von Zeichen, um die der Parameter `Mindestlänge` verringert wird, wenn im Kennwort mindestens ein Kleinbuchstabe enthalten ist.
- `GB_Bonus` ist die Anzahl von Zeichen, um die der Parameter `Mindestlänge` verringert wird, wenn im Kennwort mindestens ein Großbuchstabe enthalten ist.
- `Z_Bonus` ist die Anzahl von Zeichen, um die der Parameter `Mindestlänge` verringert wird, wenn im Kennwort mindestens eine Ziffer enthalten ist.
- `AZ_Bonus` ist die Anzahl der Zeichen, um die der Parameter `Mindestlänge` verringert wird, wenn der Anwender mindestens ein Sonderzeichen wie z. B. einen Unterstrich oder einen Bindestrich verwendet.

Geben Sie die Zeichenbonus-Parameter als positive Zahl oder, wenn der Anwender keinen Bonus für diese Zeichenklasse erhalten soll, als „0“ an. Die Zeichenboni werden addiert. Je mehr verschiedene Zeichenarten der Anwender eingibt, desto weniger Zeichen sind notwendig, um ein gültiges Kennwort zu erstellen. Beispiel:

```
esxcfg-auth --usecrack=3 11 1 1 1 2
```

Mit dieser Einstellung benötigt ein Anwender, der ein Kennwort aus Kleinbuchstaben und einem Unterstrich erstellt, acht Zeichen, um ein gültiges Kennwort zu erstellen. Wenn der Anwender hingegen alle Zeichenarten (Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen) einfügt, benötigt er nur sechs Zeichen.

Änderung des Kennwort-Plug-Ins

Für die meisten Umgebungen ist das Plug-In `pam_cracklib.so` zur Durchsetzung einer ordnungsgemäßen Kennwortqualität ausreichend. Wenn `pam_cracklib.so` jedoch nicht Ihren Bedürfnissen entspricht, können Sie auch das Plug-In `pam_passwdqc.so` verwenden. Sie können das Plug-In über den Befehl `esxcfg-auth` ändern.

Das Plug-In `pam_passwdqc.so` überprüft die gleichen Kennwortmerkmale wie `pam_cracklib.so`. Es bietet jedoch mehr Optionen zur Feinabstimmung der Kennwortqualität und führt für alle Anwender einschließlich des Root-Anwenders Kennwortqualitätstests durch. Die Verwendung von `pam_passwdqc.so` ist jedoch auch etwas komplizierter als die Verwendung von `pam_cracklib.so`. Weitere Informationen zu diesem Plug-In finden Sie in der Linux-Dokumentation.

HINWEIS Das pam_passwdqc.so-Plug-In, das unter Linux verwendet wird, verfügt über mehr Parameter als das Plug-In für ESX Server. Diese zusätzlichen Parameter können nicht mit esxcfg-auth eingerichtet werden.

Wechseln zum Plug-In pam_passwdqc.so

1 Melden Sie sich auf der Servicekonsole an und erlangen Sie Root-Privilegien.

2 Geben Sie den folgenden Befehl ein:

```
esxcfg-auth --usepamqc=<N0> <N1> <N2> <N3> <N4> <Übereinstimmung>
```

Wobei:

- N0 die Anzahl der Zeichen ist, die für ein Kennwort notwendig sind, das nur aus Zeichen einer Zeichenklasse gebildet wird.
- N1 die Anzahl der Zeichen ist, die für ein Kennwort notwendig sind, das aus Zeichen von zwei Zeichenklassen gebildet wird.
- N2 für Kennwortsätze verwendet wird. Für ESX Server sind mindestens drei Wörter notwendig, um einen Kennwortsatz zu bilden.
- N3 die Anzahl der Zeichen ist, die für ein Kennwort notwendig sind, das aus Zeichen von drei Zeichenklassen gebildet wird.
- N4 die Anzahl der Zeichen ist, die für ein Kennwort notwendig sind, das aus Zeichen von allen vier Zeichenklassen gebildet wird.
- Übereinstimmung die Anzahl der Zeichen ist, die in einer Zeichenfolge wiederverwendet wird, die aus dem alten Kennwort stammt. Wenn pam_passwdqc.so eine wiederverwendete Zeichenfolge mit mindestens dieser Länge findet, schließt es diese Zeichenfolge aus dem Qualitätstest aus und verwendet zur Prüfung nur die übrigen Zeichen.

Wenn eine dieser Optionen auf -1 gesetzt wird, ignoriert pam_passwdqc.so diese Anforderung. Wenn eine dieser Optionen auf disabled (deaktiviert) gesetzt wird, lehnt pam_passwdqc.so das Kennwort mit einem entsprechenden Merkmal ab. Die Werte müssen in absteigender Reihenfolge verwendet werden; ausgenommen hiervon sind -1 und disabled.

Beispiel:

```
esxcfg-auth --usepamqc=disabled 18 -1 12 8
```

In dieser Einstellung werden alle Kennwörter, die ein Anwender erstellt und die nur eine Zeichenklasse enthalten, abgelehnt. Ein Kennwort mit zwei Zeichenklassen müsste mindestens 18 Zeichen lang sein, ein Kennwort mit drei Zeichenklassen 12 Zeichen lang und ein Kennwort mit vier Zeichenklassen 8 Zeichen lang. Versuche zur Erstellung eines Kennwortsatzes werden ignoriert.

Schlüsselqualität

Die Übertragung von Daten über unsichere Verbindungen stellt ein Sicherheitsrisiko dar, da böswillige Anwender Daten scannen können, während sie im Netzwerk übertragen werden. Als Schutz dagegen verschlüsseln die Netzwerkkomponenten meistens die Daten, sodass diese nicht so einfach gelesen werden können. Zur Verschlüsselung verwendet die Quellkomponente, zum Beispiel eine Gateway, Algorithmen, sog. *Schlüssel*, um die Daten zu ändern, bevor sie übertragen werden. Die Zielkomponenten verwendet dann einen Schlüssel, um die Daten zu entschlüsseln und sie in ihre ursprüngliche Form zu bringen.

Derzeit werden verschiedene Schlüssel verwendet; die Sicherheitsebene jedes dieser Chiffren ist unterschiedlich. Ein Maß zur Bestimmung der Datenschutzfähigkeit eines Schlüssels ist die *Schlüsselqualität* – die Anzahl der Bits im Verschlüsselungsschlüssel. Je höher diese Anzahl ist, desto sicherer ist der Schlüssel.

Damit die Daten aus und zu externen Netzwerken gesendeten Daten geschützt werden, verwendet ESX Server eine der sichersten Blockschlüssel, die es derzeit gibt – 256-Bit-AES-Blockverschlüsselung. ESX Server verwendet außerdem 1024-Bit-RSA für den Schlüsselaustausch. Diese Verschlüsselungsalgorithmen sind für folgende Verbindungen Standard:

- VI Client-Verbindungen zu VirtualCenter Server und zum ESX Server-Host über die Servicekonsole.
- VI-Web Access-Verbindungen zum ESX Server-Host über die Servicekonsole.

HINWEIS Da die Verwendung von Verschlüsselungstechniken für VI-Web Access vom Webbrowser abhängig ist, den Sie verwenden, verwendet dieses Management-Tool ggf. eine andere Verschlüsselung.

- SDK-Verbindungen zu VirtualCenter Server und zum ESX Server.
- Servicekonsolenverbindungen zu den virtuellen Maschinen über VMkernel.
- SSH-Verbindungen zum ESX Server-Host über die Servicekonsole. Weitere Informationen finden Sie unter „SSH-Sicherheit“ auf Seite 255.

Setuid- und setgid-Anwendungen

`setuid` ist ein Kennzeichen, mit dem eine Anwendung die Zugriffsberechtigungen eines Anwenders, der die Anwendung ausführt, ändern kann, indem es die tatsächliche Anwender-ID auf die Anwender-ID des Programmbesitzers setzt. `setgid` ist ein Kennzeichen, mit dem eine Anwendung die Zugriffsberechtigungen einer Gruppe, die die Anwendung ausführt, ändern kann, indem es die tatsächliche Gruppen-ID auf die Gruppen-ID des Programmbesitzers setzt.

Während der Installation von ESX Server werden standardmäßig verschiedene Anwendungen installiert, die das `setuid`- und `setgid`-Kennzeichen enthalten. Diese Anwendungen werden von der Servicekonsole oder über sie aufgerufen. Manche dieser Anwendungen enthalten Hilfsprogramme, die zur korrekten Ausführung des ESX Server-Hosts notwendig sind. Andere Anwendungen sind optional, erleichtern aber ggf. die Wartung und Fehlerbehebung auf dem ESX Server-Host und im Netzwerk.

setuid-Standardanwendungen

Tabelle 12-2 listet die `setuid` Standardanwendungen auf und zeigt an, ob eine Anwendung erforderlich oder optional ist.

Tabelle 12-2. `setuid` Standardanwendungen

Anwendung	Zweck und Pfad	Erforderlich oder optional
`crontab`	Ermöglicht es einzelnen Anwendern, Cron-Aufträge hinzuzufügen. **Pfad:** `/usr/bin/crontab`	Optional
`pam_timestamp_check`	Unterstützt Kennwortauthentifizierung. **Pfad:** `/sbin/pam_timestamp_check`	Erforderlich
`passwd`	Unterstützt Kennwortauthentifizierung. **Pfad:** `/usr/bin/passwd`	Erforderlich
`ping`	Versendet und wartet auf Kontrolldatenpakete auf der Netzwerkschnittstelle. Nützlich zur Problemsuche in Netzwerken. **Pfad:** `/bin/ping`	Optional
`pwdb_chkpwd`	Unterstützt Kennwortauthentifizierung. **Pfad:** `/sbin/pwdb_chkpwd`	Erforderlich
`ssh-keysign`	Zur host-basierten Authentifizierung für sichere SSH-Shells. **Pfad:** `/usr/libexec/openssh/ssh-keysign`	Erforderlich, wenn Sie host-basierte Authentifizierung verwenden. Ansonsten optional.
`su`	Macht durch Anwenderwechsel aus einem allgemeinen Anwender einen Root-Anwender. **Pfad:** `/bin/su`	Erforderlich
`sudo`	Macht aus einem allgemeinen Anwender für bestimmte Vorgänge einen Root-Anwender. **Pfad:** `/usr/bin/sudo`	Optional

Tabelle 12-2. `setuid` Standardanwendungen (Fortsetzung)

Anwendung	Zweck und Pfad	Erforderlich oder optional
`unix_chkpwd`	Unterstützt Kennwortauthentifizierung. **Pfad:** `/sbin/unix_chkpwd`	Erforderlich
`vmkload_app`	Führt Aufgaben zur Ausführung von virtuellen Maschinen aus. Diese Anwendung befindet sich an zwei Speicherorten: an einem Speicherort zur normalen Verwendung und an einem zur Fehlersuche. **Pfad für normale Verwendung:** `/usr/lib/vmware/bin/vmkload_app` **Pfad zur Fehlersuche:** `/usr/lib/vmware/bin-debug/vmkload_app`	In beiden Verzeichnissen erforderlich
`vmkping`	Versendet und wartet auf Kontrolldatenpakete auf der Netzwerkschnittstelle. Nützlich zur Problemsuche in Netzwerken. **Pfad:** `/usr/lib/vmware/bin/vmkping`	Optional
`vmware-authd`	Authentifiziert Anwender zur Verwendung bestimmter VMware Dienste. Pfad: `/usr/sbin/vmware-authd`	Erforderlich
`vmware-vmx`	Führt Aufgaben zur Ausführung von virtuellen Maschinen aus. Diese Anwendung befindet sich an zwei Speicherorten: an einem Speicherort zur normalen Verwendung und an einem zur Fehlersuche. **Pfad für normale Verwendung:** `/usr/lib/vmware/bin/vmware-vmx` **Pfad zur Fehlersuche:** `/usr/lib/vmware/bin-debug/vmware-vmk`	In beiden Verzeichnissen erforderlich

Wenn Sie eine der erforderlichen Anwendungen deaktivieren, führt dies zu Problemen bei der ESX Server-Authentifizierung und beim Betrieb der virtuellen Maschinen; Sie können jedoch alle optionalen Anwendungen deaktivieren.

Deaktivierung einer optionalen setuid-Anwendung

1 Melden Sie sich auf der Servicekonsole an und erlangen Sie Root-Privilegien.

2 Geben Sie folgenden Befehl ein:

```
chmod a-s <path_to_executable>
```

setgid-Standardanwendungen

Es werden standardmäßig zwei Anwendungen installiert, die das `setgid`-Kennzeichen enthalten. Tabelle 12-3 listet die `setgid` Standardanwendungen auf und zeigt an, ob eine Anwendung erforderlich oder optional ist.

Tabelle 12-3. `setgid` Standardanwendungen

Anwendung	Zweck und Pfad	Erforderlich oder optional
`wall`	Warnt alle Anschlüsse, dass ein bestimmter Vorgang bevorsteht. Diese Anwendung wird durch `shutdown` und andere Befehle aufgerufen. **Pfad:** `/usr/bin/wall`	Optional
`lockfile`	Führt Sperroperationen für den Dell OM-Management-Agenten aus. **Pfad:** `/usr/bin/lockfile`	Für Dell OM erforderlich, ansonsten optional

Wenn Sie eine der erforderlichen Anwendungen deaktivieren, führt dies zu Problemen bei der ESX Server-Authentifizierung und beim Betrieb der virtuellen Maschinen; Sie können jedoch alle optionalen Anwendungen deaktivieren.

Deaktivierung einer optionalen setgid-Anwendung

1 Melden Sie sich auf der Servicekonsole an und erlangen Sie Root-Privilegien.

2 Geben Sie folgenden Befehl ein:

```
chmod a-g <path_to_executable>
```

SSH-Sicherheit

SSH ist eine häufig verwendete UNIX- und Linux-Befehlsshell, mit der Sie sich aus der Ferne auf der Servicekonsole anmelden und bestimmte Management- und Konfigurationsaufgaben für ESX Server durchführen können. SSH wird für sichere Anmeldevorgänge und Datenübertragungen verwendet, weil es einen höheren Schutz als andere Befehlsshells bietet. In dieser ESX Server-Version wurde die SSH-Konfiguration verbessert, um eine noch höhere Sicherheit zu gewährleisten. Zu diesen Verbesserungen gehören unter anderem:

- **Deaktivierung des SSH-Protokolls Version 1** – VMware unterstützt das SSH-Protokoll in Version 1 nicht mehr, sondern verwendet nun ausschließlich das Protokoll in Version 2. Version 2 behebt bestimmte Sicherheitsprobleme von Version 1 und bietet eine sicherere Kommunikationsschnittstelle zur Servicekonsole.
- **Verbesserte Schlüsselqualität** – SSH unterstützt nun nur noch 256-Bit- und 128-Bit-AES-Schlüssel für Verbindungen.

- **Beschränkte Fernanmeldung als Root** – Sie können sich nicht mehr aus der Ferne als Root anmelden. Sie melden sich stattdessen als Anwender an und verwenden dann entweder den `sudo`-Befehl, um bestimmte Vorgänge, die Root-Privilegien erfordern, auszuführen, oder den Befehl `su`, um zum Root-Anwender zu werden.

HINWEIS Der `sudo`-Befehl bietet Sicherheitsvorteile, da er die Root-Aktivitäten einschränkt und es ermöglicht, den möglichen Missbrauch von Root-Privilegien zu überprüfen, indem er eine Prüfliste alle Root-Aktivitäten, die der Anwender durchführt, anlegt.

Diese Einstellungen wurden so entworfen, dass die Daten, die Sie über SSH an die Servicekonsole übertragen, gut geschützt werden. Wenn diese Konfiguration für Ihre Bedürfnisse zu streng ist, können Sie die Sicherheitsparameter senken.

Änderung der Standard-SSH-Konfiguration

1 Melden Sie sich auf der Servicekonsole an und erlangen Sie Root-Privilegien.

2 Wechseln Sie in der Eingabeaufforderung über den Befehl `cd /etc/ssh` das Verzeichnis.

3 Führen Sie mit nano oder einem anderen Texteditor nach Bedarf einen oder mehrere der folgenden Vorgänge aus.

   - Wenn Sie die Root-Fernanmeldung zulassen möchten, ändern Sie die Einstellung in der folgenden Zeile der Datei `sshd_config` auf `yes` (Ja):

     ```
     PermitRootLogin no
     ```

   - Um zum ursprünglichen SSH-Protokoll (Version 1 und 2) zurückzukehren, kommentieren Sie folgende Zeile in der Datei `sshd_config` aus:

     ```
     Protocol 2
     ```

   - Um 3DES-Verschlüsselung und andere Verschlüsselungsarten auch weiterhin zu verwenden, kommentieren Sie folgende Zeile in der Datei `sshd_config` aus:

     ```
     Ciphers aes256-cbc,aes128-cbc
     ```

   - Um Secure FTP (SFTP) auf SSH zu deaktivieren, kommentieren Sie folgende Zeile in der Datei `sshd_config` aus:

     ```
     Subsystem ftp /usr/libexec/openssh/sftp-server
     ```

4 Speichern Sie die Änderungen und schließen Sie die Datei.

5 Geben Sie folgenden Befehl ein, um den SSHD-Dienst neu zu starten:

```
service sshd restart
```

Sicherheitspatches und Sicherheitslücken-Scanner

Wenn ein Patch für ein bestimmtes von LINUX unterstütztes Software-Paket, das von VMware als Servicekonsolenkomponente angeboten wird – zum Beispiel ein Dienst, ein Hilfsprogramm oder ein Protokoll – verfügbar wird, stellt VMware ein Paket für den RPM Package Manager (RPM) zur Verfügung, mit dem Sie das Software-Paket auf ESX Server aktualisieren können. Verwenden Sie immer die RPMs, die VMware zur Verfügung stellt, selbst wenn diese Patches auch von Drittanbietern als RPM angeboten werden.

Bei der Veröffentlichung von Patches für ein Software-Paket portiert VMware den Patch grundsätzlich auf eine Version der Software zurück, die auch wirklich stabil ist. Durch diese Herangehensweise werden die Chancen verringert, dass durch den Patch neue Fehler und Stabilitätsprobleme in die Software integriert werden. Da der Patch auf eine bestehende Version der Software aufgespielt wird, bleibt die Versionsnummer der Software gleich, nur die Patchnummer wird als Suffix angehängt.

Bestimmte Sicherheitsscanner wie Nessus überprüfen zwar die Versionsnummer, nicht jedoch das Patch-Suffix, wenn sie nach Sicherheitslücken suchen. Daher kann es dazu kommen, dass diese Scanner fälschlicherweise melden, dass die Software nicht aktuell ist und - ungeachtet der Realität - nicht die aktuellsten Sicherheitspatches enthält. Dieses Problem tritt in der Branche häufig auf und ist nicht auf VMware beschränkt.

HINWEIS Einige Sicherheitsscanner sind in der Lage, diese Situation korrekt zu verarbeiten, aber normalerweise liegen sie um eine Version oder mehr zurück. So bringt die Nessus-Version, die nach einem Red Hat-Patch veröffentlicht wird, diese Fehlmeldungen meistens nicht.

Es folgt ein Beispiel, wie dieses Problem entsteht:

1. Sie installieren ESX Server mit OpenSSL Version 0.9.7a (wobei 0.9.7a die ursprüngliche Version ohne Patches ist).
2. OpenSSL veröffentlicht einen Patch, der eine Sicherheitslücke in Version 0.9.7 schließt. Diese Version wird 0.9.7x genannt.
3. VMware portiert den Patch OpenSSL 0.9.7x auf die ursprüngliche Version zurück, aktualisiert die Patchnummer und erstellt ein RPM. Die OpenSSL-Version in dem RPM ist 0.9.7a-1, d. h. die ursprüngliche Version (0.9.7a) enthält nun Patch 1.
4. Sie installieren den RPM.
5. Der Sicherheitsscanner übersieht das Suffix „-1“ und meldet fälschlicherweise, dass die Sicherheit für OpenSSL nicht aktuell ist.

Wenn Ihr Scanner meldet, dass die Sicherheit für ein Paket nicht aktuell ist, führen Sie die folgenden Überprüfungen durch:

- Überprüfen Sie das Patch-Suffix, um zu bestimmen, ob Sie eine Aktualisierung benötigen.

- Konsultieren Sie die RPM-Dokumentation von VMware bezüglich Informationen zu den Patchinhalten.
- Verwenden Sie folgenden Befehl, um die „Common Vulnerabilities and Exposures“-Nummer (CVE) aus der Sicherheitswarnung im RPM-Änderungsprotokoll nachzuschlagen:

  ```
  rpm–q ––changelog openssl | grep <CVE_Nummer>
  ```

  Wenn sich die CVE-Nummer dort befindet, deckt das Paket die Sicherheitslücke ab.

Sichere Implementierungen und Sicherheits-empfehlungen

13

Dieses Kapitel soll Ihnen eine bessere Vorstellung von der Absicherung von ESX Server in bestimmten Umgebungen vermitteln. Dazu wird eine Reihe von ESX Server-Implementierungen vorgestellt, die Ihnen bei der Planung der Sicherheitsfunktionen in Ihrer eigenen Implementierung helfen können. Außerdem enthält dieses Kapitel einige grundlegende Sicherheitsempfehlungen, die Sie bei der Erstellung und Konfiguration von virtuellen Maschinen in Betracht ziehen sollten.

In diesem Kapitel werden folgende Themen behandelt:

- „Sicherheitsmaßnahmen für häufig verwendete ESX Server-Implementierungen“ auf Seite 259
- „Empfehlungen für virtuelle Maschinen“ auf Seite 265

Sicherheitsmaßnahmen für häufig verwendete ESX Server-Implementierungen

Die Komplexität von ESX Server-Implementierungen kann je nach Größe Ihres Unternehmens, der gemeinsamen Nutzung von Daten und Ressourcen durch Außenstehende und der Verwendung eines oder mehrerer Datacenters variieren.

Zu den folgenden Implementierungen gehören Policys für den Anwenderzugriff, die gemeinsame Nutzung von Ressourcen sowie Sicherheitsstufen. Durch den Vergleich der Implementierungen können Sie die Probleme erkennen, die Sie bei der Planung der Sicherheit für Ihre eigene ESX Server-Implementierung beachten müssen.

Implementierung „Ein Kunde“

In dieser Implementierung befinden sich die ESX Server-Hosts in einem Unternehmen und einem einzigen Datacenter und werden auch dort gewartet. ESX Server-Ressourcen werden nicht durch außenstehende Anwender genutzt. Die ESX Server- Hosts werden von einem globalen Administrator unterhalten, auf den Hosts werden mehrere virtuelle Maschinen ausgeführt.

Die Implementierung lässt Kundenadministratoren nicht zu; der globale Administrator ist für die Wartung der verschiedenen virtuellen Maschinen allein verantwortlich. Das Unternehmen beschäftigt mehrere Systemadministratoren, die keine Konten auf dem ESX Server-Host haben und nicht auf ESX Server-Programme wie VirtualCenter oder Befehlszeilenshells für den Host zugreifen können. Diese Systemadministratoren haben über die VM-Konsole auf die virtuellen Maschinen Zugriff, sodass Sie Software installieren und andere Wartungsaufgaben in den virtuellen Maschinen durchführen können.

Tabelle 13-1 zeigt, wie Sie die Komponenten gemeinsam nutzen und für den ESX Server-Host konfigurieren können.

Tabelle 13-1. Gemeinsame Komponentennutzung für die Ein-Kunde-Implementierung

Funktion	Konfiguration	Anmerkungen
Servicekonsole auf dem gleichen physischen Netzwerk wie die virtuellen Maschinen?	Nein	Isolieren Sie die Servicekonsole, sodass sie über ihr eigenes physisches Netzwerk verfügt.
Servicekonsole auf dem gleichen VLAN wie die virtuellen Maschinen?	Nein	Isolieren Sie die Servicekonsole, sodass sie über ihr eigenes VLAN verfügt. Virtuelle Maschinen oder andere Systemkomponenten wie z. B. VMotion sollten ein anderes VLAN verwenden.
Virtuelle Maschinen im gleichen physischen Netzwerk?	Ja	Die virtuellen Maschinen nutzen das gleiche physische Netzwerk.
Gemeinsame Netzwerkadapternutzung?	Teilweise	Isolieren Sie die Servicekonsole, sodass sie über ihren eigenen virtuellen Switch und virtuellen Netzwerkadapter verfügt. Virtuelle Maschinen oder andere Systemkomponenten sollten einen anderen Switch oder Adapter verwenden. Die virtuellen Maschinen können sich jedoch einen virtuellen Switch oder Netzwerkadapter teilen.
Gemeinsame VMFS-Nutzung?	Ja	Alle `.vmdk`-Dateien sollten sich auf der gleichen VMFS-Partition befinden.
Sicherheitsstufe	Hoch	Geben Sie Ports für benötigte Dienste wie z. B. FTP nach Bedarf frei. Weitere Informationen zu den Sicherheitsstufen finden Sie unter „Konfiguration der Servicekonsolen-Firewall“ auf Seite 240.
Speichermehrfachvergabe für virtuelle Maschinen?	Ja	Der konfigurierte Gesamtspeicher für die virtuellen Maschinen kann größer als der physische Gesamtspeicher sein.

Tabelle 13-2 Die folgende Tabelle zeigt, wie die Anwenderkonten für den ESX Server-Host eingerichtet werden können.

Tabelle 13-2. Anwenderkonten in einer Ein-Kunden-Implementierung

Anwenderkategorie	Gesamtanzahl der Konten
Globale Administratoren	1
Kundenadministratoren	0
Systemadministratoren	0
Unternehmensanwender	0

Tabelle 13-3 Die folgende Tabelle zeigt die Zugriffsberechtigungen für die Anwender.

Tabelle 13-3. Anwenderzugriff in einer Ein-Kunden-Implementierung

Zugriffsbefugnisse	Globaler Administrator	Systemadministrator
Root-Zugriff?	Ja	Nein
Servicekonsolenzugriff über SSH?	Ja	Nein
VirtualCenter und VI-Web Access?	Ja	Nein
Erstellung und Änderung von virtuellen Maschinen?	Ja	Nein
Zugriff auf virtuelle Maschinen über die Konsole?	Ja	Ja

Implementierung für mehrere Kunden mit Beschränkungen

In dieser Implementierung befinden sich die ESX Server-Hosts im gleichen Datacenter und werden für Anwendungen mehrerer Kunden verwendet. Der globale Administrator wartet die ESX Server-Hosts, auf denen mehrere virtuelle Maschinen jeweils für die einzelnen Kunden ausgeführt werden. Die virtuellen Maschinen der verschiedenen Kunden können sich auf dem gleichen ESX Server-Host befinden, aber der globale Administrator beschränkt die gemeinsame Nutzung von Ressourcen, um die Datensicherheit zu gewährleisten.

Es gibt einen globalen Administrator und mehrere Kundenadministratoren, die die virtuellen Maschinen ihrer jeweiligen Kunden warten. Zu dieser Implementierung gehören auch Systemadministratoren der Kunden, die kein ESX Server-Konto haben, aber über die VM-Konsole auf die virtuellen Maschinen zugreifen können, um Software zu installieren und andere Wartungsaufgaben auf den virtuellen Maschinen durchzuführen.

Tabelle 13-4 zeigt, wie Sie die Komponenten gemeinsam nutzen und für den ESX Server-Host konfigurieren können.

Tabelle 13-4. Gemeinsame Komponentennutzung in einer Implementierung für mehrere Kunden mit Beschränkungen

Funktion	Konfiguration	Anmerkungen
Servicekonsole auf dem gleichen physischen Netzwerk wie die virtuellen Maschinen?	Nein	Isolieren Sie die Servicekonsole, sodass sie über ihr eigenes physisches Netzwerk verfügt.
Servicekonsole auf dem gleichen VLAN wie die virtuellen Maschinen?	Nein	Isolieren Sie die Servicekonsole, sodass sie über ihr eigenes VLAN verfügt. Virtuelle Maschinen oder andere Systemkomponenten wie z. B. VMotion sollten ein anderes VLAN verwenden.
Virtuelle Maschinen im gleichen physischen Netzwerk?	Teilweise	Installieren Sie die virtuellen Maschinen jedes Kunden auf einem anderen physischen Netzwerk. Alle physischen Netzwerke sind voneinander unabhängig.
Gemeinsame Netzwerkadapternutzung?	Teilweise	Isolieren Sie die Servicekonsole, sodass sie über ihren eigenen virtuellen Switch und virtuellen Netzwerkadapter verfügt. Virtuelle Maschinen oder andere Systemkomponenten sollten einen anderen Switch oder Adapter verwenden. Die virtuellen Maschinen eines Kunden können den gleichen virtuellen Switch und Netzwerkadapter haben. Sie sollten sich jedoch Switch und Adapter nicht mit anderen Kunden teilen.
Gemeinsame VMFS-Nutzung?	Nein	Jeder Kunde hat seine eigene VMFS-Partition, die `.vmdk`-Dateien der virtuellen Maschinen befinden sich ausschließlich auf dieser Partition. Diese Partition kann mehrere LUNs umfassen.
Sicherheitsstufe	Hoch	Geben Sie Ports für Dienste wie FTP nach Bedarf frei.
Speichermehrfachvergabe für virtuelle Maschinen?	Ja	Der konfigurierte Gesamtspeicher für die virtuellen Maschinen kann größer als der physische Gesamtspeicher sein.

Tabelle 13-5 Die folgende Tabelle zeigt, wie die Anwenderkonten für den ESX Server-Host eingerichtet werden können.

Tabelle 13-5. Anwenderkonten in einer Implementierung für mehrere Kunden mit Beschränkungen

Anwenderkategorie	Gesamtanzahl der Konten
Globale Administratoren	1
Kundenadministratoren	10
Systemadministratoren	0
Unternehmensanwender	0

Tabelle 13-6 Die folgende Tabelle zeigt die Zugriffsberechtigungen für die Anwender.

Tabelle 13-6. Anwenderzugriff in einer Implementierung für mehrere Kunden mit Beschränkungen

Zugriffsbefugnisse	Globaler Administrator	Kundenad-ministrator	Systemad-ministrator
Root-Zugriff?	Ja	Nein	Nein
Servicekonsolenzugriff über SSH?	Ja	Ja	Nein
VirtualCenter und VI-Web Access?	Ja	Ja	Nein
Erstellung und Änderung von virtuellen Maschinen?	Ja	Ja	Nein
Zugriff auf virtuelle Maschinen über die Konsole?	Ja	Ja	Ja

Implementierung für mehrere Kunden ohne Beschränkungen

In dieser Implementierung befinden sich die ESX Server-Hosts im gleichen Datacenter und werden für Anwendungen mehrerer Kunden verwendet. Der globale Administrator wartet die ESX Server-Hosts, auf denen mehrere virtuelle Maschinen jeweils für die einzelnen Kunden ausgeführt werden. Die virtuellen Maschinen der verschiedenen Kunden können sich auf dem gleichen ESX Server-Host befinden, aber es gibt weniger Beschränkungen zur gemeinsamen Nutzung von Ressourcen.

Es gibt einen globalen Administrator und mehrere Kundenadministratoren, die die virtuellen Maschinen ihrer jeweiligen Kunden warten. Zu dieser Implementierung gehören auch Systemadministratoren der Kunden, die kein ESX Server-Konto haben, aber über die VM-Konsole auf die virtuellen Maschinen zugreifen können, um Software zu installieren und andere Wartungsaufgaben auf den virtuellen Maschinen durchzuführen. Außerdem kann eine Gruppe von Unternehmensanwendern ohne Konten die virtuellen Maschinen zur Ausführung ihrer Anwendungen verwenden.

Tabelle 13-7 zeigt, wie Sie die Komponenten gemeinsam nutzen und für den ESX Server-Host konfigurieren können.

Tabelle 13-7. Gemeinsame Komponentennutzung in einer Implementierung für mehrere Kunden ohne Beschränkungen

Funktion	Konfiguration	Anmerkungen
Servicekonsole auf dem gleichen physischen Netzwerk wie die virtuellen Maschinen?	Nein	Isolieren Sie die Servicekonsole, sodass sie über ihr eigenes physisches Netzwerk verfügt.
Servicekonsole auf dem gleichen VLAN wie die virtuellen Maschinen?	Nein	Isolieren Sie die Servicekonsole, sodass sie über ihr eigenes VLAN verfügt. Virtuelle Maschinen oder andere Systemkomponenten wie z. B. VMotion sollten ein anderes VLAN verwenden.
Virtuelle Maschinen im gleichen physischen Netzwerk?	Ja	Die virtuellen Maschinen nutzen das gleiche physische Netzwerk.
Gemeinsame Netzwerkadapternutzung?	Teilweise	Isolieren Sie die Servicekonsole, sodass sie über ihren eigenen virtuellen Switch und virtuellen Netzwerkadapter verfügt. Virtuelle Maschinen oder andere Systemkomponenten sollten einen anderen Switch oder Adapter verwenden. Alle virtuellen Maschinen können sich einen virtuellen Switch oder Netzwerkadapter teilen.
Gemeinsame VMFS-Nutzung?	Ja	Die virtuellen Maschinen können VMFS-Partitionen gemeinsam nutzen, die `.vmdk`-Dateien der virtuellen Maschinen können sich auf einer gemeinsamen Partition befinden. Die virtuellen Maschinen verwenden keine gemeinsamen `.vmdk`-Dateien.
Sicherheitsstufe	Hoch	Geben Sie Ports für Dienste wie FTP nach Bedarf frei.
Speichermehrfachvergabe für virtuelle Maschinen?	Ja	Der konfigurierte Gesamtspeicher für die virtuellen Maschinen kann größer als der physische Gesamtspeicher sein.

Tabelle 13-8 Die folgende Tabelle zeigt, wie die Anwenderkonten für den ESX Server-Host eingerichtet werden können.

Tabelle 13-8. Anwenderkonten in einer Implementierung für mehrere Kunden ohne Beschränkungen

Anwenderkategorie	Gesamtanzahl der Konten
Globale Administratoren	1
Kundenadministratoren	10
Systemadministratoren	0
Unternehmensanwender	0

Tabelle 13-9 Die folgende Tabelle zeigt die Zugriffsberechtigungen für die Anwender.

Tabelle 13-9. Anwenderzugriff in einer Implementierung für mehrere Kunden ohne Beschränkungen

Zugriffsbefugnisse	Globaler Administrator	Kundenad-ministrator	Systemad-ministrator	Unter-nehmensan-wender
Root-Zugriff?	Ja	Nein	Nein	Nein
Servicekonsolenzu-griff über SSH?	Ja	Ja	Nein	Nein
VirtualCenter und VI-Web Access?	Ja	Ja	Nein	Nein
Erstellung und Än-derung von virtuellen Maschinen?	Ja	Ja	Nein	Nein
Zugriff auf virtuelle Maschinen über die Konsole?	Ja	Ja	Ja	Ja

Empfehlungen für virtuelle Maschinen

Beachten Sie bei der Einschätzung der Sicherheit von virtuellen Maschinen und bei der Verwaltung von virtuellen Maschinen folgende Sicherheitsmaßnahmen.

Installation von Antiviren-Software.

Da auf jeder virtuellen Maschine ein Standardbetriebssystem ausgeführt wird, sollten Sie es durch die Installation von Antiviren-Software gegen Viren schützen. Je nach Verwendungszweck der virtuellen Maschine sollte ggf. auch eine Firewall installiert werden.

HINWEIS Firewalls und Antiviren-Software können die Virtualisierungsleistung beeinflussen. Wenn Sie sich sicher sind, dass sich die virtuellen Maschinen in einer vollständig vertrauenswürdigen Umgebung befinden, können Sie diese beiden Sicherheits-maßnahmen gegen Leistungsnachteile abwägen.

Deaktivierung von Kopiervorgängen zwischen Gast-Betriebssystem und Remote-Steuerung

Wenn VMware Tools auf einer virtuellen Maschine ausgeführt wird, können Sie Kopiervorgänge mit Kopieren/Einfügen zwischen dem Gast-Betriebssystem und der Remote-Steuerung ausführen. Sobald das Konsolenfenster angebunden wurde, können unbefugte Anwender und Prozesse in der virtuellen Maschine auf die Zwischenablage der VM-Konsole zugreifen. Wenn ein Anwender vor der Benutzung der Konsole geheime Informationen in die Zwischenablage kopiert, macht der Anwender der virtuellen Maschine - vielleicht unwissentlich - geheime Daten zugänglich.

Um dies zu verhindern, können Sie Kopiervorgänge für das Gast-Betriebssystem deaktivieren.

Deaktivierung von Kopiervorgängen zwischen Gast-Betriebssystem und Remote-Steuerung

1 Melden Sie sich am VI Client an und wählen Sie die virtuelle Maschine aus dem Inventar aus.

   Die Konfiguration für diese virtuelle Maschine wird mit der Registerkarte **Übersicht** angezeigt.

2 Klicken Sie auf **Einstellungen bearbeiten**.

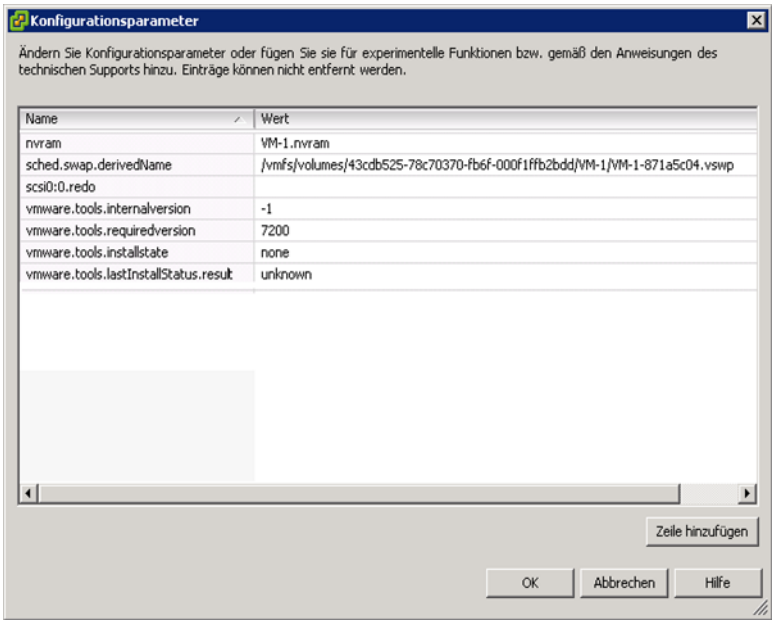
3 Klicken Sie auf **Optionen** > **Erweitert** > **Konfigurationsparameter**. Das Dialogfeld **Konfigurationsparameter** wird geöffnet.

4 Klicken Sie auf die Schaltfläche **Hinzufügen**.

5 Geben Sie in der Spalte **Wert** für **Name** folgende Werte ein.

Name	Wert
`isolation.tools.copy.enable`	`Falsch`
`isolation.tools.paste.enable`	`Falsch`
`isolation.tools.setGUIOptions.enable`	`Falsch`

Das Ergebnis sieht folgendermaßen aus.



HINWEIS Diese Optionen heben die Einstellungen in der Systemsteuerung von VMware Tools auf dem Gast-Betriebssystem auf.

6 Klicken Sie auf **OK**, um das Dialogfeld **Konfigurationsparameter** zu schließen, und dann noch einmal auf **OK**, um das Dialogfeld **Eigenschaften der virtuellen Maschinen** zu schließen.

Entfernung überflüssiger Hardware-Geräte

Anwender und Prozesse ohne Befugnisse in der virtuellen Maschine können Hardware-Geräte wie Netzwerkadapter oder CD-ROM-Laufwerke einbinden oder trennen. Angreifer können diese Fähigkeit auf verschiedene Arten nutzen, um die Sicherheit einer virtuellen Maschine anzugreifen. So kann zum Beispiel ein Angreifer mit Zugang zu einer virtuellen Maschine folgende Angriffe durchführen:

- Eibindung eines nicht verbundenen CD-ROM-Laufwerks und Zugriff auf Informationen auf dem Medium, das sich im Laufwerk befindet.
- Trennung eines Netzwerkadapters, um die virtuelle Maschine vom Netzwerk zu isolieren, was zu einem Ausfall führt.

Als allgemeine Sicherheitsmaßnahme sollten Sie Befehle auf dem Registerkarte „Konfiguration“ auf dem VI Client verwenden, um alle nicht benötigten oder ungenutzten Hardware-Geräte zu entfernen. Zwar erhöht diese Maßnahme die Sicherheit der virtuellen Maschinen, aber sie ist keine gute Lösung, wenn ein gegenwärtig ungenutztes Gerät später reaktiviert werden soll.

Wenn Sie ein Gerät nicht dauerhaft entfernen möchten, können Sie verhindern, dass ein Anwender oder Prozess einer virtuellen Maschine das Gerät aus dem Gast-Betriebssystem heraus einbindet oder trennt.

Schutz vor dem Trennen von Geräten durch einen Anwender oder Prozess auf einer virtuellen Maschine

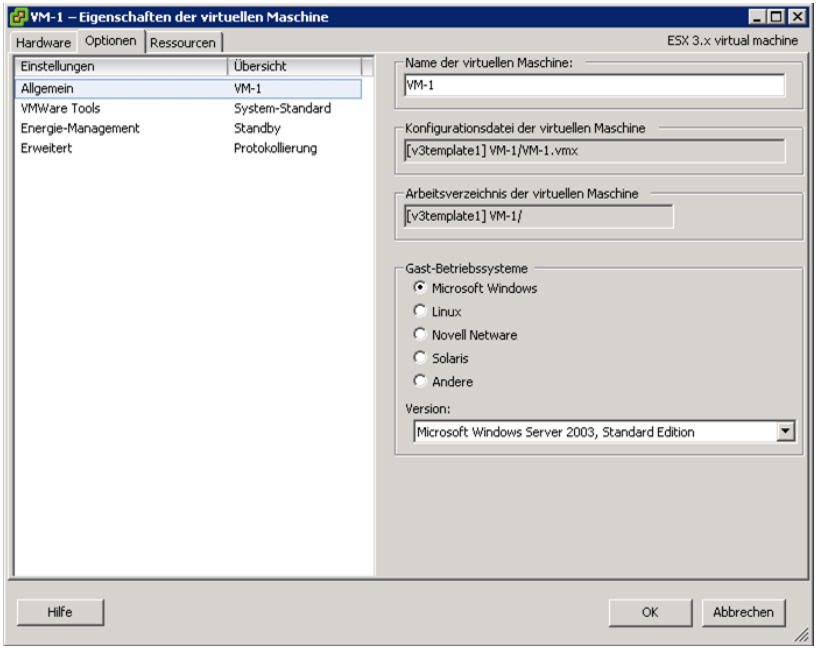
1 Melden Sie sich am VI Client an und wählen Sie die virtuelle Maschine aus dem Inventar aus.

   Die Konfiguration für diese virtuelle Maschine wird mit der Registerkarte **Übersicht** angezeigt.

2 Klicken Sie auf **Einstellungen bearbeiten**.

   Das Dialogfeld **Eigenschaften der virtuellen Maschine** wird geöffnet.

3 Klicken Sie auf **Einstellungen** > **Allgemeines** und notieren Sie sich den Pfad, der im Feld **Konfigurationsdatei der virtuellen Maschine** angezeigt wird.



4 Melden Sie sich auf der Servicekonsole an und erlangen Sie Root-Privilegien.

5 Wechseln Sie in das Verzeichnis, um auf die Konfigurationsdatei der virtuellen Maschine zuzugreifen, deren Pfad Sie sich in Schritt Schritt 3 notiert haben.

Die Konfigurationsdateien der virtuellen Maschinen befinden sich im Verzeichnis `/vmfs/volumes/<datastore>`, wo es sich beim `<datastore>` um den Namen des Speicher-Gerätes handelt, auf dem die Dateien der virtuellen Maschine gespeichert sind. Wenn beispielsweise die Konfigurationsdatei der virtuellen Maschine, die Sie aus dem Dialogfeld **Eigenschaften der virtuellen Maschine** erhalten haben, `[vol1]vm-finance/vm-finance.vmx` entspricht, wechseln Sie die Verzeichnisse wie folgt:

```
cd /vmfs/volumes/vol1/vm–finance/
```

6 Verwenden Sie Nano oder einen anderen Text-Editor, um die `.vmx` Datei um die folgende Zeile zu ergänzen.

```
<device_name>.allowGuestConnectionControl = “false”
```

Wobei `<device_name>` der Name des Gerätes ist, das geschützt werden soll, z. B. ethernet1.

HINWEIS Standardmäßig ist Ethernet 0 so konfiguriert, dass die Trennung des Geräts nicht möglich ist. Der einzige Grund, aus dem Sie veranlasst sein können, dies zu ändern, ergibt sich dann, wenn ein ehemaliger Administrator den `<device_name>.allowGuestConnectionControl` auf `True` gesetzt hat.

7 Speichern Sie die Änderungen und schließen Sie die Datei.

8 Kehren Sie zum VI Client zurück und schalten Sie die virtuelle Maschine erst aus und dann wieder an. Dazu klicken Sie mit der rechten Maustaste auf die virtuelle Maschine im Inventarfenster und klicken auf **Ausschalten** und anschließend auf **Einschalten**.

Verhinderung von Flooding des ESX Server-Hosts durch Prozesse des Gast-Betriebssystems

Die Prozesse des Gast-BetriebssystemGast-Betriebssystems senden über VMware Tools informative Meldungen an den ESX Server-Host. Diese Meldungen, die `setinfo`-Meldungen genannt werden, enthalten normalerweise Name-Wert-Paare zu Merkmalen von virtuellen Maschinen oder Bezeichnern, die der Host speichert, – zum Beispiel `ipaddress=10.17.87.224`.

Eine `setinfo`-Meldung hat kein vorgegebenes Format und kann beliebig lang sein. Daher ist die Datenmenge, die auf diese Weise an den Host weitergeleitet werden kann, unbegrenzt. Ein unbeschränkter Datenstrom bietet Angreifern eine gute Möglichkeit, über eine Software, die VMware Tools imitiert, einen DOS-Angriff zu starten, indem der Host mit Paketen überflutet wird, durch die Ressourcen belegt werden, die von den virtuellen Maschinen benötigt werden.

Um dieses Problem zu verhindern, kann die Fähigkeit von VMware Tools beschränkt werden, willkürlich `setinfo`-Meldungen an den ESX Server-Host zu schicken.

HINWEIS VMware Tools sendet auch andere Meldungen, aber diese verfügen über festgelegte Formate und sind daher nicht so gut für DOS-Angriffe geeignet.

Verhinderung willkürlicher Meldungen von Prozessen des Gast-Betriebssystems an den Host

1 Melden Sie sich am VI Client an und wählen Sie die virtuelle Maschine aus dem Inventar aus.

Die Konfiguration für diese virtuelle Maschine wird mit der Registerkarte **Übersicht** angezeigt.

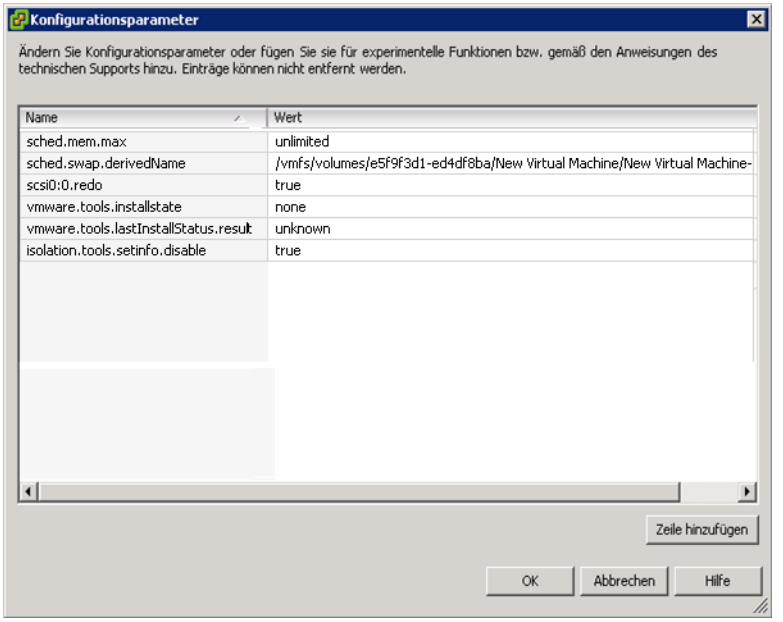
2 Klicken Sie auf **Einstellungen bearbeiten**.

3 Klicken Sie auf **Optionen** > **Erweitert** > **Konfigurationsparameter**. Das Dialogfeld **Konfigurationsparameter** wird geöffnet.

4 Klicken Sie auf die Schaltfläche **Hinzufügen** und geben Sie Folgendes ein:

- **Namenfeld** – `isolation.tools.setinfo.disable`
- **Wertfeld** – TRUE

Das Ergebnis sieht folgendermaßen aus.



5 Klicken Sie auf **OK**, um das Dialogfeld **Konfigurationsparameter** zu schließen, und dann noch einmal auf **OK**, um das Dialogfeld **Eigenschaften der virtuellen Maschinen** zu schließen.

Deaktivierung der Protokollierung für das Gast-Betriebssystem

Virtuelle Maschinen können Informationen zur Fehlerbehebung in eine Protokolldatei der virtuellen Maschine, die auf dem VMFS-Datenträger gespeichert wird, schreiben. Anwender und Prozesse von virtuellen Maschinen können die Protokollierung entweder absichtlich oder unabsichtlich missbrauchen, sodass große Datenmengen die Protokolldatei überfluten. Mit der Zeit kann die Protokolldatei so genug Speicherplatz im Dateisystem der Servicekonsole belegen, um einen Ausfall zu verursachen.

Um dieses Problem zu verhindern, können Sie die Protokollierung für die Gastbetriebssysteme von virtuellen Maschinen deaktivieren. Beachten Sie, dass Sie in diesem Fall ggf. nicht in der Lage sind, entsprechende Protokolle für die Fehlerbehebung zu sammeln. Außerdem leistet VMware keine technische Unterstützung für virtuelle Maschinen, bei denen die Protokollierung deaktiviert wurde.

Deaktivierung der Protokollierung für das Gast-Betriebssystem

1 Melden Sie sich am VI Client an und wählen Sie die virtuelle Maschine aus dem Inventar aus.

Die Konfiguration für diese virtuelle Maschine wird mit der Registerkarte **Übersicht** angezeigt.

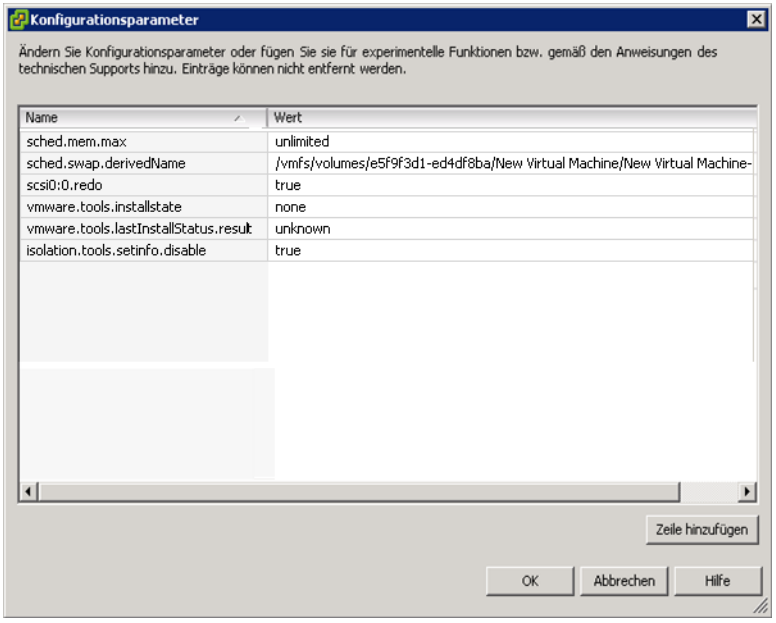
2 Klicken Sie auf **Einstellungen bearbeiten**.

3 Klicken Sie auf **Optionen** > **Erweitert** > **Konfigurationsparameter**. Das Dialogfeld **Konfigurationsparameter** wird geöffnet.

4 Klicken Sie auf die Schaltfläche **Hinzufügen** und geben Sie Folgendes ein:

- **Namenfeld** – `isolation.tools.log.disable`
- **Wertfeld** – `TRUE`

Das Ergebnis sieht folgendermaßen aus.



5 Klicken Sie auf **OK**, um das Dialogfeld **Konfigurationsparameter** zu schließen, und dann noch einmal auf **OK**, um das Dialogfeld **Eigenschaften der virtuellen Maschinen** zu schließen.

Anhänge

ESX-Befehle zur technischen Unterstützung

A

Dieser Anhang führt die Befehle der Servicekonsole aus, die dazu verwendet werden, den ESX Server zu konfigurieren. Die meisten dieser Befehle sind nur für die Verwendung durch die technische Unterstützung vorgesehen und hier nur zu rein informativen Zwecken aufgeführt. In einigen wenigen Fällen sind diese Befehle jedoch das einzige Mittel zur Ausführung einer bestimmten Konfigurationsaufgabe für den ESX Server-Host. Auch wenn die Verbindung zum Host unterbrochen wird, bleibt Ihnen nur die Ausführung einiger dieser Befehle über die Befehlszeilenoberfläche – zum Beispiel, wenn das Netzwerk ausfällt und der Zugriff über den VI Client daher nicht verfügbar ist.

HINWEIS Wenn Sie die Befehle in diesem Anhang verwenden, müssen Sie den Befehl `service mgmt-vmware restart` ausführen, um den Prozess `vmware-hostd` neu zu starten und den VI Client und andere Verwaltungs-Tools auf die Änderungen der Konfiguration aufmerksam zu machen. Im Allgemeinen sollten Sie die Ausführung der Befehle aus diesem Anhang vermeiden, wenn der Host gerade durch den VI Client oder den VirtualCenter Server verwaltet wird.

Die grafische Benutzeroberfläche des VI Clients ist das bevorzugte Mittel zur Ausführung der Konfigurationsaufgaben, die in diesem Anhang beschrieben werden. Sie können diesen Anhang verwenden, wenn Sie wissen möchten, welche VI Client-Befehle anstelle der Servicekonsolenbefehle verwendet werden können. Dieser Anhang fasst die Aktionen, die Sie in VI Client durchführen, zusammen, bietet jedoch keine vollständige Anleitung. Details zur Verwendung der Befehle und zur Ausführung von Konfigurationsaufgaben über den VI Client finden Sie in der Online-Hilfe.

Zusätzliche Informationen zu bestimmten ESX-Befehlen erhalten Sie, wenn Sie sich auf der Servicekonsole anmelden und sich die man-Seiten mit dem Befehl `man <esxcfg_Befehlsname>` anzeigen lassen.

Tabelle A-1 Führt die Befehle für den technischen Support für den ESX Server auf, fasst den Zweck jedes Befehls zusammen und bietet eine Alternative zum VI Client. Sie

können die meisten der VI Client-Vorgänge, die in der Tabelle aufgeführt werden, erst dann ausführen, wenn Sie einen ESX Server-Host aus dem Inventar ausgewählt und auf die Registerkarte **Konfiguration** geklickt haben. Dies muss vor der Ausführung der unten aufgeführten Prozeduren durchgeführt werden, sofern nichts anderes angegeben wurde.

Tabelle A-1. Befehle für die technische Unterstützung von ESX Server

Servicekonsolenbefehl	Zweck des Befehls und VI Client-Verfahren
`esxcfg-advcfg`	Konfiguriert erweiterte Optionen für ESX Server. Um die erweiterten Optionen im VI Client zu konfigurieren, klicken Sie auf **Erweiterte Einstellungen**. Wenn das Dialogfeld **Erweiterte Einstellungen** geöffnet wird, verwenden Sie die Liste auf der linken Seite, um den Gerätetyp oder die Aktivität auszuwählen, mit dem/der Sie arbeiten möchten und nehmen Sie die entsprechenden Einstellungen vor.
`esxcfg-auth`	Konfiguriert die Authentifizierung. Verwenden Sie diesen Befehl, um zwischen den Plug-Ins `pam_cracklib.so` und `pam_passwdqc.so` zur Durchsetzung der Änderungsregeln für Kennwörter umzuschalten. Mit diesem Befehl können Sie auch die Optionen für diese beiden Plug-Ins zurücksetzen. Weitere Informationen finden Sie unter „Kennwort-Komplexität“ auf Seite 246. Diese Funktionen können im VI Client nicht konfiguriert werden.
`esxcfg-boot`	Konfiguriert die Bootstrap-Einstellungen. Dieser Befehl wird für den Bootstrap-Prozess verwendet und ist nur für die technische Unterstützung von VMware vorgesehen. Geben Sie diesen Befehl nur auf ausdrückliche Anweisung eines Vertreters der technischen Unterstützung von VMware ein. Diese Funktionen können im VI Client nicht konfiguriert werden.
`esxcfg-dumppart`	Konfiguriert eine Diagnosepartition oder sucht nach bestehenden Diagnosepartitionen. Bei der Installation von ESX Server wird eine Diagnosepartition zur Speicherung von Informationen zur Fehlersuche erstellt, wenn ein Systemfehler auftritt. Sie müssen diese Partition nicht manuell anlegen, es sei denn, Sie stellen fest, dass es keine Diagnose-Partition für den Host gibt. Für Diagnosepartitionen stehen im VI Client folgende Verwaltungsvorgänge zur Verfügung: ■ **Vorhandensein einer Diagnosepartition** – Klicken Sie auf **Storage** (Speicher) > **Hinzufügen** und überprüfen Sie die erste Seite des **Assistenten zum Hinzufügen von Speicher**, ob dort die Option **Diagnose** aufgeführt wird. Wenn **Diagnose** nicht zu den Optionen zählt, verfügt ESX Server bereits über eine Diagnosepartition. ■ **Konfiguration einer Diagnosepartition** – Klicken Sie auf **Speicher** > **Hinzufügen** > **Diagnose** und folgen Sie den Anweisungen des Assistenten.

Tabelle A-1. Befehle für die technische Unterstützung von ESX Server (Fortsetzung)

Servicekonsolenbefehl	Zweck des Befehls und VI Client-Verfahren
`esxcfg-firewall`	Konfiguriert die Ports der Servicekonsolen-Firewall. Wählen Sie zur Konfiguration der Firewall-Ports für unterstützte Dienste und Assistenten im VI Client die Internet-Dienste aus, die auf den ESX Server-Host zugreifen dürfen. Klicken Sie auf **Sicherheitsprofil** > **Firewall** > **Eigenschaften** und fügen Sie über das Dialogfeld **Firewall-Eigenschaften** Dienste hinzu. Weitere Informationen zum Hinzufügen von Diensten und zur Konfiguration von Firewalls finden Sie unter „Freigeben von Firewall-Ports für unterstützte Dienste und Management-Agenten“ auf Seite 192. Sie können den VI Client nicht dazu verwenden, nicht-unterstützte Dienste zu konfigurieren. Verwenden Sie für diese Dienste den `esxcfg-firewall` Befehl, wie in „Konfiguration der Servicekonsolen-Firewall“ auf Seite 240 beschrieben.
`esxcfg-info`	Druckt Informationen zum Status der Servicekonsole, des VMkernels, verschiedener Untersysteme im virtuellen Netzwerk und zur Speicherressourcen-Hardware aus. Mit dem VI Client können diese Informationen nicht ausgedruckt werden, die meisten Informationen können jedoch über verschiedene Registerkarten und Funktionen in der Benutzeroberfläche gewonnen werden. So können Sie zum Beispiel den Status der virtuellen Maschinen über die Registerkarte **Virtuelle Maschinen** überprüfen.
`esxcfg-init`	Führt interne Initialisierungsroutinen aus. Dieser Befehl wird für den Bootstrap-Prozess verwendet und Sie sollten ihn unter keinen Umständen ausführen. Dieser Befehl kann zu Problemen mit dem ESX Server-Host führen. Es gibt keine VI Client-Entsprechung für diesen Befehl.
`esxcfg-linuxnet`	Konvertiert beim Start von ESX Server `vswif` in `eth`, wodurch der Modus „Nur Servicekonsole“ statt der ESX-Modus gestartet wird. Dieser Befehl wird für den Bootstrap-Prozess verwendet und ist nur für die technische Unterstützung von VMware vorgesehen. Geben Sie diesen Befehl nur auf ausdrückliche Anweisung eines Vertreters der technischen Unterstützung von VMware ein. Es gibt keine VI Client-Entsprechung für diesen Befehl.
`esxcfg-module`	Legt die Treiber-Parameter fest und ändert die Einstellung, welche Treiber während des Hochfahrens geladen werden. Dieser Befehl wird für den Bootstrap-Prozess verwendet und ist nur für die technische Unterstützung von VMware vorgesehen. Geben Sie diesen Befehl nur auf ausdrückliche Anweisung eines Vertreters der technischen Unterstützung von VMware ein. Es gibt keine VI Client-Entsprechung für diesen Befehl.
`esxcfg-mpath`	Konfiguriert die Multipath-Einstellungen für Fibre-Channel- oder iSCSI-Festplatten. Klicken Sie zur Konfiguration der Multipath-Einstellungen für den Speicher im VI Client auf **Speicher**. Wählen Sie einen Datastore oder eine zugeordnete LUN aus und klicken Sie auf **Eigenschaften**. Wählen Sie ggf. im Dialogfeld **Eigenschaften** die gewünschte Erweiterung aus. Klicken Sie dann auf **Bereichsgerät** > **Pfade verwalten** und konfigurieren Sie die Pfade über das Dialogfeld **Pfad verwalten**.

Tabelle A-1. Befehle für die technische Unterstützung von ESX Server (Fortsetzung)

Servicekonsolenbefehl	Zweck des Befehls und VI Client-Verfahren
`esxcfg-nas`	Verwaltet die NAS-Einbindung. Mit diesem Befehl können Sie NAS-Geräte hinzufügen, löschen, auflisten oder ihre Attribute ändern. Klicken Sie zur Anzeige der NAS-Geräte im VI Client auf **Speicher** und blättern Sie durch das Speicherverzeichnis. Aus der **Speicher**-Ansicht können Sie außerdem folgende Vorgänge ausführen: ■ **Attribute eines NAS-Gerätes anzeigen** – Markieren Sie das Gerät. Sie erhalten die Daten unter **Details**. ■ **Hinzufügen eines NAS-Geräts** – Klicken Sie auf **Speicher hinzufügen**. ■ **Löschen eines NAS-Gerätes** – Klicken Sie auf **Entfernen**. ■ **Änderung der Attribute eines NAS-Gerätes** – Klicken Sie auf das Gerät und dann auf **Details** > **Eigenschaften**. Eine vollständige Anleitung zur Erstellung und Konfiguration von NAS-Datastores erhalten Sie unter „Konfiguration von ESX Server zum Zugriff auf NFS-Datenträger“ auf Seite 135.
`esxcfg-nics`	Druckt ein Verzeichnis der physischen Netzwerkadapter sowie Informationen zum Treiber, dem PCI-Gerät und dem Verbindungsstatus jeder NIC. Sie können diesen Befehl auch verwenden, um die Geschwindigkeit und den Duplexmodus eines physischen Netzwerkadapters zu steuern. Die Informationen zu den physischen Netzwerkadaptern des Hosts können Sie im VI Client anzeigen, indem Sie auf **Network Adapters** (Netzwerkadapter) klicken. Klicken Sie zur Änderung der Geschwindigkeit und des Duplexmodus für einen physischen Netzwerkadapter im VI Client bei einem virtuellen Switch, der dem physischen Netzwerkadapter zugeordnet wurde, auf **Netzwerk** > **Eigenschaften**. Klicken Sie dann im Dialogfeld **Eigenschaften** auf **Network Adapters** (Netzwerkadapter) > **Bearbeiten** und wählen Sie die Geschwindigkeit/Duplex aus. Weitere Informationen zur Änderung der Geschwindigkeit und des Duplexmodus finden Sie unter „Konfiguration der Geschwindigkeit des Uplink-Netzwerkadapters“ auf Seite 49.
`esxcfg-resgrp`	Stellt die Ressourcen-Gruppeneinstellungen wieder her und ermöglicht die Ausführung grundlegender Verwaltungsaufgaben für Ressourcen-Gruppen. Wählen Sie einen Ressourcen-Pool aus dem Inventarfenster aus und klicken Sie auf **Einstellungen bearbeiten** in der **Übersicht-**Registerkarte, um die Einstellungen der Ressourcen-Gruppe zu ändern.
`esxcfg-route`	Legt die Standard-Gatewayroute des VMkernels fest oder ändert sie. Um die Standard-Gatewayroute des VMkernels im VI Client festzulegen, klicken Sie auf **DNS und Routing**. Wenn Sie die Standardroute ändern möchten, klicken Sie auf **Eigenschaften** und aktualisieren Sie die Daten auf beiden Registerkarten im Dialogfeld **DNS- und Routing-Konfiguration**.

Tabelle A-1. Befehle für die technische Unterstützung von ESX Server (Fortsetzung)

Servicekonsolenbefehl	Zweck des Befehls und VI Client-Verfahren
`esxcfg-swiscsi`	Konfiguriert den Software-iSCSI-Software-Adapter. Klicken Sie zur Konfiguration des Software-iSCSI-Systems im VI Client auf **Speicheradapter**, markieren Sie den iSCSI-Adapter, den Sie konfigurieren möchten, und klicken Sie auf **Eigenschaften**. Konfigurieren Sie den Adapter über das Dialogfeld **Eigenschaften des iSCSI-Initiators**. Eine vollständige Anleitung zur Erstellung und Konfiguration von iSCSI-Datastores erhalten Sie unter „iSCSI-Speicher“ auf Seite 110.
`esxcfg-upgrade`	Aktualisiert ESX Server von ESX Server 2.*x* auf ESX Server 3.*x*. Dieser Befehl ist nicht zur allgemeinen Verwendung bestimmt. Durch die Aktualisierung von 2.*x* auf 3.*x* werden die folgenden drei Ziele erreicht. Einige davon können im VI Client ausgeführt werden: ■ **Aktualisierung des Hosts** – Bei der Aufrüstung von ESX Server 2.*x* auf ESX Server 3.*x* werden die Binärdateien aktualisiert. Diesen Schritt können Sie nicht über den VI Client ausführen. Informationen zur Durchführung dieser Aktualisierung erhalten Sie im *Installations- und Upgrade-Handbuch*. ■ **Aktualisierung des Dateisystems** – Wenn Sie VMFS-2 auf VMFS-3 aktualisieren möchten, halten Sie Ihre virtuellen Maschinen an oder fahren Sie sie herunter und klicken Sie dann auf **Inventar** > **Host** > **In den Wartungsmodus wechseln**. Klicken Sie auf **Speicher**, wählen Sie ein Speichergerät aus und klicken Sie auf **Auf VMFS-3 aktualisieren**. Sie müssen diesen Schritt für jedes Speichergerät ausführen, das Sie aktualisieren möchten. ■ **Upgrade der virtuellen Maschinen** – Um eine virtuelle Maschine von VMS-2 auf VMS-3 zu aktualisieren, klicken Sie mit der rechten Maustaste auf die virtuelle Maschine im Inventarfenster und wählen Sie **Upgrade der virtuellen Maschine durchführen**.
`esxcfg-vmhbadevs`	Druckt eine Zuordnung von VMkernel-Speichergeräten auf Servicekonsolengeräte. Es gibt keine VI Client-Entsprechung für diesen Befehl.
`esxcfg-vmknic`	Erstellt und aktualisiert VMkernel-TCP/IP-Einstellungen für VMotion, NAS und iSCSI. Klicken Sie zur Einrichtung von Netzwerkverbindungen von VMotion, NFS oder iSCSI im VI Client auf **Netzwerk** > **Vernetzen**. Wählen Sie **VMkernel** aus und folgen Sie den Anweisungen des **Assistenten zum Hinzufügen von Netzwerken**. Definieren Sie die IP-Adresse-Subnetzmask und den VMkernel-Standardgateway im Schritt **Verbindungseinstellungen**. Wenn Sie die Einstellungen überprüfen möchten, klicken Sie auf das blaue Symbol links neben dem VMotion-, iSCSI- oder NFS-Port. Wenn Sie eine der Einstellungen bearbeiten möchten, klicken Sie für den entsprechenden Switch auf **Eigenschaften**. Wählen Sie den Port aus dem Verzeichnis im Dialogfeld **Eigenschaften** aus und klicken Sie auf **Bearbeiten**, um den das **Eigenschaften** Dialogfeld zum Port zu öffnen und die Einstellungen für den Port zu ändern. Eine vollständige Anleitung zur Erstellung und Aktualisierung von Netzwerkverbindungen für VMotion, NFS oder iSCSI finden Sie unter „Konfiguration des VMkernels“ auf Seite 33.

Tabelle A-1. Befehle für die technische Unterstützung von ESX Server (Fortsetzung)

Servicekonsolenbefehl	Zweck des Befehls und VI Client-Verfahren
`esxcfg-vswif`	Erstellt und aktualisiert die Netzwerkeinstellungen der Servicekonsole. Dieser Befehl wird verwendet, wenn Sie den ESX Server-Host aufgrund von Problemen mit der Netzwerkkonfiguration nicht über den VI Client verwalten können. Weitere Informationen finden Sie unter „Fehlerbehebung bei der Vernetzung der Servicekonsole“ auf Seite 80. Klicken Sie zur Einrichtung von Netzwerkverbindungen für die Servicekonsole im VI Client auf **Netzwerk > Vernetzen**. Wählen Sie **Servicekonsole** aus und folgen Sie den Anweisungen des **Assistent zum Hinzufügen von Netzwerken**. Im Schritt **Verbindungseinstellungen** wird die IP-Adressen-Subnetzmaske und der Standardgateway der Servicekonsole eingerichtet. Wenn Sie die Einstellungen überprüfen möchten, klicken Sie auf das blaue Symbol links vom Servicekonsolen-Port. Wenn Sie eine der Einstellungen bearbeiten möchten, klicken Sie für den entsprechenden Switch auf **Eigenschaften**. Wählen Sie den Servicekonsolen-Port aus der Liste des Dialogfelds zu den Switch-**Eigenschaften** aus. Klicken Sie auf **Bearbeiten**, um die **Eigenschaften** des Ports zu öffnen und dessen Einstellungen zu ändern. Eine vollständige Anleitung zur Erstellung und Aktualisierung der Servicekonsolenverbindung finden Sie unter „Konfiguration der Servicekonsole“ auf Seite 37.
`esxcfg-vswitch`	Erstellt und aktualisiert die Netzwerkeinstellungen für virtuelle Maschinen. Klicken Sie zur Einrichtung von Netzwerkverbindungen für eine virtuelle Maschine im VI Client auf **Netzwerk > Vernetzen**. Wählen Sie **Virtuelle Maschine** aus und folgen Sie den Anweisungen des **Assistent zum Hinzufügen von Netzwerken**. Wenn Sie die Einstellungen überprüfen möchten, klicken Sie auf das Sprechblasen-Symbol links von der gewünschten Port-Gruppe der virtuellen Maschine. Wenn Sie eine der Einstellungen bearbeiten möchten, klicken Sie für den entsprechenden Switch auf **Eigenschaften**. Wählen Sie den Port der virtuellen Maschine aus dem Verzeichnis im Dialogfeld **Eigenschaften** aus und klicken Sie auf **Bearbeiten**, um das Dialogfeld Port **Eigenschaften** zu öffnen und dessen Einstellungen zu ändern. Eine vollständige Anleitung zur Erstellung und Aktualisierung von virtuellen Maschinen finden Sie unter „Konfiguration virtueller Netzwerke für virtuelle Maschinen“ auf Seite 29.

Andere Befehle

Um bestimmte interne Vorgänge zu unterstützen, enthalten die ESX Server Installationen eine Reihe von Standard Linux Konfigurationsbefehlen, wie beispielsweise Befehle zur Konfiguration von Netzwerken und Speichern. Eine Verwendung dieser Befehle zur Ausführung von Konfigurationstasks kann zu schwerwiegenden Konfigurationskonflikten führen und auch dazu, dass bestimmte ESX Server Funktionen nicht weiter verwendet werden können. Arbeiten Sie immer mit dem VI Client, um den ESX Server zu konfigurieren, es sei denn, die VMware Infrastruktur Dokumentation oder der technische Support von VMware erteilen Ihnen andere Anweisungen.

Verwendung von vmkfstools

B

Sie verwenden das vmkfstools Programm, um virtuelle Festplatten, Dateisysteme, logische Volumen und physische Speicher-Geräte auf dem VMware ESX Server anzulegen und einzurichten. Mit vmkfstools können Sie das VMware Dateisystem (VMDS) auf einer physischen Partition auf einer Festplatte anlegen und verwalten. Sie können dieses Programm auch dazu verwenden, Dateien, wie z. B. virtuelle Festplatten zu bearbeiten, die auf VMFS-2, VMFS-3 und NFS gespeichert sind.

Die meisten vmkfstools-Vorgänge können auch über den VI Client ausgeführt werden. Weitere Informationen zur Verwendung des VI Clients zur Speicherverwaltung finden Sie unter „Speicherkonfiguration“ auf Seite 103.

Dieser Anhang behandelt die folgenden Abschnitte:

- „vmkfstools-Befehlssyntax“ auf Seite 282
- „vmkfstools-Optionen“ auf Seite 283
- „Beispiele für die Verwendung von vmkfstools“ auf Seite 295

vmkfstools-Befehlssyntax

Im Allgemeinen müssen Sie sich nicht als der Root-Benutzer anmelden, um die `vmkfstools` Befehle auszuführen. Manche Befehle jedoch, wie zum Beispiel die Befehle zum Dateisystem, erfordern eine Root-Anmeldung.

Verwenden Sie mit dem `vmkfstools` Befehl die folgenden Argumente:

- Bei `<options>` handelt es sich um eine oder mehrere Befehlszeilenoptionen und zugeordnete Argumente, die Sie dazu verwenden, die Aktivität anzugeben, die `vmkfstools` ausführen soll – wie beispielsweise, die Auswahl des Festplattenformats beim Erstellen einer neuen virtuellen Festplatte.

  Nach der Eingabe dieser Option, geben Sie eine Datei oder ein VMFS-Dateisystem an, auf dem Sie den Vorgang ausführen möchten, indem Sie einen relativen oder absoluten Datei-Pfadnamen in der `/vmfs` Hierarchie eingeben.

- `<Partition>` bezeichnet die Festplatten-Partitionen. Dieses Argument verwendet ein `vmhbaA:T:L:P` Format, in dem es sich bei `A`, `T`, `L` und `P` um Ganzzahlen handelt, die den Adapter, das Target, die LUN und die Partitionsnummer bezeichnen. Diese Zahl der Partition muss größer als Null sein und muss der gültigen VMFS-Partition des Typs `fb` entsprechen.

  `vmhba0:2:3:1` beispielsweise bezieht sich auf die erste Partition auf LUN 3, Target 2, HBA 0.

- `<device>` bezeichnet Geräte oder logische Volumen. Das Argument verwendet einen Pfadnamen im ESX Server Geräte-Dateisystem. Der Pfadname beginnt mit `/vmfs/devices`, wobei es sich um den Mount Point des Geräte-Dateisystems handelt.

  Verwenden Sie zur Angabe der verschiedenen Gerätetypen die folgenden Formate:

  - `/vmfs/devices/disks` für lokale oder SAN-basierte Festplatten.
  - `/vmfs/devices/lvm` für logische ESX Server Volumen.
  - `/vmfs/devices/generic` für generische SCSI-Geräte, wie zum Beispiel Bandlaufwerke.

- `<path>` bezeichnet ein VMFS-Dateisystem oder eine Datei. Bei diesem Argument handelt es sich um einen absoluten oder relativen Pfad, der einen symbolischen Link zu einem Verzeichnis, dem Raw Device Mapping oder eine Datei unter `/vmfs` aufführt.

  - Um ein VMFS-Dateisystem anzugeben, verwenden Sie dieses Format:

    ```
    /vmfs/volumes/<file_system_UUID> oder
                  /vmfs/volumes/<file_system_label>
    ```

- Um eine VMFS-Datei anzugeben, verwenden Sie dieses Format:

  ```
  /vmfs/volumes/<file system label|file system UUID>/[dir]/myDisk.vmdk
  ```

  Sie brauchen nicht den gesamten Pfad anzugeben, wenn das aktuelle Arbeitsverzeichnis gleichzeitig das übergeordnete Verzeichnis von `myDisk.vmdk` ist.

Beispiel:

```
/vmfs/volumes/datastore1/rh9.vmdk
```

Suboption -v

Die Suboption `-v` bestimmt die Ausführlichkeit der Meldungen in der Befehlsausgabe. Das Format für diese Suboption lautet wie folgt:

```
-v --verbose <Zahl>
```

Der Wert `<Zahl>` wird als ganze Zahl von 1 bis 10 angegeben.

Sie können die Suboption `-v` für alle `vmkfstools`-Optionen verwenden. Wenn die Suboption `-v` für die Ausgabe einer Option nicht vorgesehen ist, ignoriert `vmkfstools` den Teil `-v` der Befehlszeile.

HINWEIS Da Sie die Suboption `-v` in jeder vmkfstools-Befehlszeile verwenden können, wird sie nicht in den Beschreibungen der einzelnen Optionen verwendet.

vmkfstools-Optionen

Dieser Abschnitt enthält eine Liste aller Optionen, die für den Befehl `vmkfstools` verwendet werden können. Einige der Aufgaben in diesem Abschnitt enthalten Optionen, die nur für Anwender mit fortgeschrittenen Kenntnissen bestimmt sind.

Die Lang- und Kurz-(Ein-Buchstaben-) formen der Optionen sind gleichwertig. So sind zum Beispiel die folgenden Befehle identisch:

```
vmkfstools --createfs vmfs3 --blocksize 2m vmhba1:3:0:1
vmkfstools -C vmfs3 -b 2m vmhba1:3:0:1
```

Weitere Informationen finden Sie in folgenden Abschnitten:

- „Dateisystemoptionen“ auf Seite 284
- „Optionen für virtuelle Festplatten“ auf Seite 287
- „Geräteoptionen“ auf Seite 294

Dateisystemoptionen

Dateisystemoptionen sind Aufgaben, die Sie bei der Einrichtung eines VMFS-Dateisystems ausführen können. Diese Einstellungen gelten nicht für NFS. Sie können einige dieser Aufgaben auch über den VI Client ausführen.

Weitere Informationen finden Sie in folgenden Abschnitten:

- „Erstellen eine VMFS-Dateisystems“ auf Seite 284
- „Erweiterung eines bestehenden VMFS-3-Volumens“ auf Seite 285
- „Auflistung der Attribute eines VMFS-Datenträgers“ auf Seite 286
- „Upgrade von VMFS-2 auf VMFS-3“ auf Seite 286

Erstellen eine VMFS-Dateisystems

```
–C ––createfs vmfs3
        –b ––blocksize <block_size>kK|mM
        –S ––setfsname <fsName>
```

Mit dieser Option wird ein VMFS-3-Dateisystem auf der angegebenen SCSI-Partition erstellt, z. B. `vmhba1:0:0:1`. Diese Partition wird die vorgelagerte Partition des Dateisystems.

HINWEIS VMFS-2-Dateisysteme sind auf ESX Server 3 schreibgeschützt. Anwender können VMFS-2-Dateisysteme nicht erstellen oder ändern, aber die darauf gespeicherten Dateien können angesehen werden. Ein Zugriff über ESX 2.x Hosts auf die VMFS-3-Datei-Systeme ist nicht möglich.

VORSICHT Beachten Sie, dass pro LUN nur ein VMFS-Datenträger möglich ist.

Für die Option `-C` können Sie folgende Suboptionen angeben:

- `-b --blocksize` – Definiert die Blockgröße für das VMFS-3-Dateisystem. Die Standard-Datei-Blockgröße beträgt 1 MB. Der <block_size>-Wert, den Sie eingeben, muss entweder 1 MB, 2 MB, 4 MB oder 8 MB betragen. Wenn Sie die Größe angeben, müssen Sie auch die Einheit als Suffix `m` oder `M` angeben. Die Größeneinheit kann klein- oder großgeschrieben werden –`vmkfstools` interpretiert sowohl `m` als auch `M` als Megabyte.
- `-S --setfsname` – Definiert die Datenträgerbezeichnung eines VMFS-Datenträgers für das VMFS-3-Dateisystem, das Sie erstellen. Verwenden Sie diese Zusatzoption nur in Verbindung mit der `-C` Option. Die Bezeichnung kann bis zu 128 Zeichen lang sein und darf keine Leerstellen am Anfang oder Ende enthalten.

  Wenn Sie die Datenträgerbezeichnung festgelegt haben, können Sie sie bei der Angabe des VMFS-Datenträgers im Befehl `vmkfstools` verwenden. Sie können die

Datenträgerbezeichnung auch verwenden, wenn Sie in den Konfigurationsdateien der virtuellen Maschine auf den Datenträger verweisen. Der Datenträgername erscheint auch in den Auflistungen, die mit dem Linux-Befehl `ls -l` und als symbolische Verknüpfung zum VMFS-Datenträger im Verzeichnis `/vmfs/volumes`.

Verwenden Sie den Linux-Befehl `ln -sf`, wenn Sie die VMFS-Datenträgerbezeichnungen ändern möchten. Beispiel:

```
ln –sf /vmfs/volumes/<UUID> /vmfs/volumes/<fsName>
```

`<fsName>` ist die neue Datenträgerbezeichnung, die Sie für die `<UUID>` des VMFS verwenden möchten.

Beispiel

```
vmkfstools –C vmfs3 –b 1m –S myvmfs vmhba1:3:0:1
```

Dieses Beispiel zeigt die Erstellung eines neuen VMFS-3-Dateisystems mit dem Namen `myvmfs` auf der ersten Partition von Target 3, LUN 0 des vmhba-Adapters 1. Die Datei-Blockgröße beträgt 1 MB.

Erweiterung eines bestehenden VMFS-3-Volumens

```
–Z ––extendfs <Erweiterungsgerät> <bestehender_VMFS–Datenträger>
```

Diese Option fügt einem vorher erstellten VMFS-Datenträger, `<bestehender VMFS-Datenträger>` eine Erweiterung hinzu. Bei jeder Verwendung dieser Option wird der VMFS-3-Datenträger um eine neue Erweiterung vergrößert, sodass der Datenträger mehrere Partitionen umfasst. Ein logischer VMFS-3-Datenträger kann bis zu 32 physische Erweiterung haben.

VORSICHT Wenn Sie diese Option ausführen, gehen alle Daten, die auf dem SCSI-Gerät, das unter `<Erweiterungsgerät>` angegeben wird, gespeichert sind, verloren.

Beispiel

```
vmkfstools –Z vmhba0:1:2:4 vmhba1:3:0:1
```

Dieses Beispiel zeigt die Erweiterung eines logischen Dateisystems durch das Hinzufügen einer neuen Partition. Das erweiterte Dateisystem nimmt nun zwei Partitionen ein – `vmhba1:3:0:1` und `vmhba0:1:2:4`. In diesem Beispiel ist `vmhba1:3:0:1` der Name der übergeordneten Partition.

Auflistung der Attribute eines VMFS-Datenträgers

```
-P --queryfs
        -h --human-readable
```

Diese Option listet die Attribute des angegebenen VMFS-Datenträgers auf, wenn sie in einer Datei oder einem Verzeichnis auf diesem VMFS-Datenträger verwendet werden. Zu den aufgelisteten Attributen gehören die VMFS-Version (VMFS-2 oder VMFS-3), die Anzahl der Erweiterungen, aus denen der jeweilige Datenträger besteht, die Datenträgerbezeichnung (falls vorhanden), die UUID und ein Verzeichnis der Gerätenamen, auf denen sich die Erweiterungen des VMFS-Datenträgers befinden.

HINWEIS Wenn ein Gerät zur Sicherung des VMFS-Dateisystems offline geht, ändert sich die Anzahl der Erweiterungen und des verfügbaren Speichers entsprechend.

Sie können die Suboption `-h` für die `-P`-Option verwenden. In diesem Fall listet `vmkfstools` die Kapazität des Datenträgers in verständlicherer Form auf – zum Beispiel `5k`, `12.1M` oder `2.1G`.

Upgrade von VMFS-2 auf VMFS-3

Sie können ein Upgrade des Dateisystems VMFS-2 auf VMFS-3 durchführen.

VORSICHT

- Die Konvertierung von VMFS-2 in VMFS-3 ist nicht umkehrbar. Wenn der VMFS-Datenträger in VMFS-3 konvertiert wurde, kann er nicht in das Format VMFS-2 zurückkonvertiert werden.
- Damit das Upgrade des Dateisystems VMFS-2 möglich ist, sollte die Dateiblockgröße nicht über 8 MB hinausgehen.

Verwenden Sie folgende Optionen für das Upgrade des Dateisystems:

- `-T --tovmfs3`
  `-x --upgradetype [zeroedthick|eagerzeroedthick|thin]`

  Diese Option konvertiert das VMFS-2-Dateisystem in VMFS-3 und erhält alle Dateien auf dem Dateisystem. Vor der Verwendung dieser `-T` Option, deinstallieren Sie die VMFS2- und VMFS3-Treiber und installieren Sie den zusätzlichen Dateisystem-Treiber, fsaux, mit der Modul-Option `fsauxFunction=upgrade`.

  Verwenden Sie die `-x --upgradetype [zeroedthick|eagerzeroedthick|thin]` Suboption mit der `-T` Option:

  - `-x zeroedthick` (default) – Behält die Eigenschaften der großen VMFS-2-Dateien. Mit dem `zeroedthick` Dateiformat, wird den Dateien zur künftigen Nutzung ein Speicherplatz zugewiesen und die nicht verwendeten Datenblöcke werden nicht entfernt.

- `-x eagerzeroedthick` – Entfernt während der Konvertierung unbenutzte Datenblöcke in großen Dateien. Wenn Sie diese Suboption verwenden, dauert das Upgrade unter Umständen wesentlich länger, als mit den anderen Optionen.
- `-x thin` – Konvertiert große VMFS-2-Dateien in kleinere, bereitgestellte VMFS-3-Dateien. Im Gegensatz zum Thick-File-Format, ermöglicht das Thin-Format es den Dateien nicht, für künftige Nutzungen einen zusätzlichen Speicherplatz zu verwenden, sondern stellt den Speicher nach Bedarf zur Verfügung. Während der Konvertierung werden unverwendete Blöcke der großen Dateien gelöscht.

Während der Konvertierung stellt der Sperr-Mechanismus des ESX Servers sicher, dass keine lokalen Prozesse auf das VMFS-Volume zugreifen, das konvertiert wird. Sie müssen gleichzeitig sicherstellen, dass kein Remote-ESX Server auf dieses Volume zugreift. Die Konvertierung kann mehrere Minuten dauern. Die Fertigstellung wird durch die Rückkehr zur Befehlszeileneingabe signalisiert.

Nach der Konvertierung deinstallieren Sie den fsaux-Treiber und installieren Sie die VMFS3 und VMFS2 Treiber, um den üblichen Betrieb wieder aufzunehmen.

- `-u --upgradefinish`

  Diese Option beendet das Upgrade.

Optionen für virtuelle Festplatten

Bei den Optionen der virtuellen Festplatten handelt es sich um Tasks, die Sie während des Einrichtens, der Migration und der Verwaltung virtueller Festplatten ausführen können, die auf den Dateisystemen VMFS-2, VMFS-3 und NFS gespeichert sind. Sie können auch die meisten dieser Aufgaben auch über den VI Client ausführen.

Weitere Informationen finden Sie in folgenden Abschnitten:

- „Unterstützte Festplattenformate“ auf Seite 288
- „Erstellen einer virtuellen Festplatte“ auf Seite 289
- „Initialisierung einer virtuellen Festplatte“ auf Seite 289
- „Vergrößern einer schlanken virtuellen Festplatte“ auf Seite 290
- „Löschen einer virtuellen Festplatte“ auf Seite 290
- „Umbenennen einer virtuellen Festplatte“ auf Seite 290
- „Klonen einer virtuellen oder Raw-Festplatte“ auf Seite 290
- „Migrieren der VMware Workstation und der VMware GSX Server virtuellen Maschinen“ auf Seite 291
- „Erweitern einer virtuellen Festplatte“ auf Seite 291

- „Migrieren einer VMFS-2 virtuellen Festplatte auf VMFS-3“ auf Seite 291
- „Anlegen einer Raw Device Mapping-Datei im virtuellen Kompatibilitätsmodus“ auf Seite 292
- „Aufführen der Attribute eines RDM“ auf Seite 292
- „Anlegen einer Raw Device Mapping-Datei im physischen Kompatibilitätsmodus“ auf Seite 293
- „Anlegen einer Deskriptor-Datei für ein Raw-Gerät“ auf Seite 293
- „Anzeige der Architektur der virtuellen Festplatte“ auf Seite 293

Unterstützte Festplattenformate

Beim Erstellen oder Klonen von virtuellen Festplatten können Sie die `-d --diskformat` Suboption verwenden, um das Format Ihrer Festplatte anzugeben. Wählen Sie ein geeignetes Format aus:

- `zeroedthick` (Standardeinstellung) – Der Speicher, den die virtuelle Festplatte benötigt, wird während des Anlegens zugewiesen. Alle Daten, die auf dem physischen Gerät verbleiben, werden nicht während des Anlegens, sondern zu einem späteren Zeitpunkt während der Lese- und Schreibvorgänge der virtuellen Maschine gelöscht.
- `eagerzeroedthick` – Der Speicher, den die virtuelle Festplatte benötigt, wird während des Anlegens zugewiesen. Im Gegensatz zum `zeroedthick`-Format, werden die verbleibenden Daten auf dem physischen Gerät während des Anlegens gelöscht. Das Anlegen von Festplatten in diesem Format kann wesentlich länger dauern, als das Anlegen von anderen Festplattentypen.
- `thick` – Der Speicher, den die virtuelle Festplatte benötigt, wird während des Anlegens zugewiesen. Bei dieser Art der Formatierung werden alten Daten gelöscht, die sich auf dem zugewiesenen Speicher befinden können.
- `thin` – Schlank-bereitgestellte (Thin-provisioned) virtuelle Festplatte. Im Gegensatz zum `Thick` Format wird der erforderliche Speicher für die virtuelle Festplatte nicht während des Anlegens bereitgestellt, sondern später in gelöschter Form und nach Bedarf.
- `rdm` – Virtueller Kompatibilitätsmodus des Raw-Disk-Mappings.
- `rdmp` – Physischer Kompatibilitätsmodus (Pass-Through) des Raw-Disk-Mappings.
- `raw` – Raw-Device.
- `2gbsparse` – Eine Ersatzfestplatte mit höchstens 2 GB Erweiterungsgröße. Festplatten in diesem Format können mit anderen VMware Produkten verwendet werden.

HINWEIS Die einzigen Festplattenformate, die für NFS verwendet werden können, sind `thin` und `2gbsparse`. Standardmäßig werden alle Dateien und virtuellen Festplatten im `Thin`-Format auf NFS-Servern gespeichert und die Blöcke bei Bedarf zugewiesen. Auf NFS werden keine anderen Optionen - auch nicht Raw-Device-Maps (RDM) unterstützt.

Erstellen einer virtuellen Festplatte

```
-c --createvirtualdisk <Größe>[kK|M|G]
        -a --adaptertype [buslogic|lsilogic]<srcfile>
        -d --diskformat [thin|zeroedthick|thick|eagerzeroedthick]
```

Diese Option erstellt eine virtuelle Festplatte auf dem angegebenen Pfad auf einem VMFS-Datenträger. Sie müssen die Größe der virtuellen Festplatte angeben. Wenn Sie für `<Größe>` einen Wert angeben, können Sie die Einheit festlegen, indem Sie entweder den Suffix `k` (Kilobyte) `m` (Megabyte) oder `g` (Gigabyte) angeben. Die Größeneinheit kann klein- oder großgeschrieben werden – `vmkfstools` interpretiert sowohl `k` als auch `K` als Kilobyte. Wenn Sie keine Einheit eingeben, ist die Standardeinstellung für `vmkfstools` Byte.

Für die `-c` Option können Sie folgende Suboptionen angeben.

- `-c` Diese Option gibt den Gerätetreiber an, der für die Kommunikation mit den virtuellen Festplatten verwendet wird. Sie haben die Auswahl zwischen den SCSI-Treibern von BusLogic und LSI Logic.
- `-d` Bezeichnet die Festplattenformate. Eine detaillierte Beschreibung des Festplattenformats finden Sie unter „Unterstützte Festplattenformate“ auf Seite 288.

Beispiel

```
vmkfstools -c 2048m /vmfs/volumes/myVMFS/rh6.2.vmdk
```

Dieses Beispiel zeigt die Erstellung einer virtuellen Festplattendatei mit dem Namen `rh6.2.vmdk` auf dem VMFS-Dateisystem mit dem Namen myVMFS. Diese Datei stellt eine leere virtuelle Festplatte dar, virtuelle Maschinen können darauf zugreifen.

Initialisierung einer virtuellen Festplatte

```
-w --writezeros
```

Mit dieser Option wird die virtuelle Festplatte bereinigt, indem die gesamten Daten mit Null überschrieben werden. In Abhängigkeit der Größe Ihrer virtuellen Festplatte und der E/A-Bandbreite des Geräts, das den Host der virtuellen Festplatte bildet, kann die Ausführung dieses Befehls lange dauern.

VORSICHT Bei der Ausführung dieses Befehls werden alle vorhandenen Daten auf der virtuellen Festplatte gelöscht.

Vergrößern einer schlanken virtuellen Festplatte

```
-j --inflatedisk
```

Mit dieser Option wird eine schlanke virtuelle Festplatte in eine Eagerzeroedthick-Festplatte konvertiert, wobei alle bestehenden Daten erhalten bleiben. Alle Blöcke, die am Anfang nicht zugewiesen wurden, werden zugewiesen und gelöscht.

Weitere Informationen zu Festplattenformaten finden Sie unter „Unterstützte Festplattenformate“ auf Seite 288.

Löschen einer virtuellen Festplatte

```
-U --deletevirtualdisk
```

Diese Option löscht Dateien unter dem angegebenen Pfad auf dem VMFS-Datenträger, die einer virtuellen Festplatte zugeordnet sind.

Umbenennen einer virtuellen Festplatte

```
-E --renamevirtualdisk <Quelldatei> <Zieldatei>
```

Diese Option benennt eine Datei einer virtuellen Festplatte, die in der Pfadangabe der Befehlszeile angegeben wird, um. Damit diese -E Option funktionieren kann, müssen Sie den ursprünglichen Dateinamen oder Dateipfad <oldName> und den neuen Dateinamen oder Pfadnamen <newName> angeben.

Klonen einer virtuellen oder Raw-Festplatte

```
-i --importfile <Quelldatei>
    -d --diskformat [rdm:<Gerät>|rdmp:<Gerät>|raw:<device>|thin|2gbsparse]
```

Diese Option erstellt eine Kopie einer virtuellen oder Raw-Festplatte, die Sie angeben.

Sie können die -d Suboption für die -i Option verwenden. Diese Suboption bezeichnet das Festplattenformat für die Kopie, die Sie anlegen. Eine detaillierte Beschreibung des Festplattenformats finden Sie unter „Unterstützte Festplattenformate“ auf Seite 288.

HINWEIS Um die ESX Server Redo-Protokolls unter Beibehaltung Ihrer Hierarchie zu klonen, verwenden Sie den cp Befehl.

Beispiel

```
vmkfstools -i /vmfs/volumes/templates/gold-master.vmdk
              /vmfs/volumes/myVMFS/myOS.vmdk
```

Dieses Beispiel zeigt das Klonen der Inhalte einer virtuellen Master-Festplatte aus dem Vorlage-Repository auf eine virtuelle Festplattendatei mit der Bezeichnung myOS.vmdk auf dem Dateisystem mit der Bezeichnung myVMFS. Sie können die virtuelle Maschine so konfigurieren, dass diese virtuelle Festplatte verwendet wird, indem Sie die folgenden Zeilen zur Konfigurationsdatei der virtuellen Maschine hinzufügen:

```
scsi0:0.present = TRUE
scsi0:0.fileName = /vmfs/volumes/myVMFS/myOS.vmdk
```

Migrieren der VMware Workstation und der VMware GSX Server virtuellen Maschinen

Sie können den VI Client nicht dazu verwenden, virtuelle Maschinen, die mit VMware Workstation oder VMware GSX Server angelegt wurden, in Ihr ESX Server System zu migrieren. Sie können jedoch den `vmkfstools -i` Befehl dazu verwenden, die virtuelle Festplatte auf Ihr ESX Server System zu migrieren und diese Festplatte dann einer neuen virtuellen Maschine hinzufügen, die Sie im ESX Server anlegen.

Migrieren der Workstation und der virtuellen GSX Server Maschinen

1 Importieren Sie eine Workstation oder GSX Server-Festplatte in Ihr `/vmfs/volumes/myVMFS/` Verzeichnis.

2 Legen Sie im VI Client eine neue virtuelle Maschine an, indem Sie die **Benutzerdefinierte** Konfigurationsoption verwenden.

3 Beim Konfigurieren der Festplatte wählen Sie die Option **Vorhandene virtuelle Festplatte verwenden** aus und fügen Sie die Workstation oder GSX Server Festplatte hinzu, die Sie importiert haben.

Erweitern einer virtuellen Festplatte

`–X ––extendvirtualdisk <Größe>[kK|M|G]`

Diese Option erweitert die Größe einer Festplatte, die einer virtuellen Maschine zugewiesen wurde, nachdem die virtuelle Maschine erstellt wurde. Die virtuelle Maschine, die diese Festplattendatei verwendet, muss bei der Eingabe dieses Befehls ausgeschaltet sein. Außerdem muss das Gast-Betriebssystem in der Lage sein, die neue Festplattengröße zu erkennen und zu verwenden, damit es z. B. das Dateisystem auf der Festplatte aktualisieren kann, sodass der zusätzliche Speicherplatz auch genutzt wird.

Wenn Sie für `Neue Größe` eine Größe angeben, können Sie die Größeneinheit festlegen, indem Sie entweder den Suffix `k` (Kilobyte), `m` (Megabyte) oder `g` (Gigabyte) angeben. Die Größeneinheit kann klein- oder großgeschrieben werden – `vmkfstools` interpretiert sowohl `k` als auch `K` als Kilobyte. Wenn Sie keine Einheit eingeben, ist die Standardeinstellung für `vmkfstools` Kilobyte.

Der Wert `Neue Größe` beschreibt die gesamte neue Größe und nicht nur die beabsichtigte Erweiterung der Festplatte.

Um beispielsweise eine 4 G virtuelle Festplatte um 1 G zu erhöhen, geben Sie Folgendes an:

vmkfstools -X 5g

Migrieren einer VMFS-2 virtuellen Festplatte auf VMFS-3

`–M ––migratevirtualdisk`

Diese Option konvertiert die angegebene virtuelle Festplattendatei vom Format ESX Server 2 ins Format ESX Server 3.

Anlegen einer Raw Device Mapping-Datei im virtuellen Kompatibilitätsmodus

`-r --createrdm <Gerät>`

Mit dieser Option wird eine Raw Device Mapping (RDM)-Datei auf einem VMFS-3 Volume angelegt und eine Raw-Festplatte dieser Datei zugeordnet. Nach Herstellung des Mappings können Sie auf die Raw-Festplatten zugreifen, wie auch auf die normalen VMFS virtuellen Festplatten. Die Dateigröße der Zuordnung entspricht der Größe der Raw-Festplatte oder Partition, auf die sie verweist.

Bei der Angabe des Werts für das `<Gerät>`, geben Sie `0` für die Partition an, was darauf hinweist, dass die gesamte Raw-Festplatte verwenden wird. Verwenden Sie das folgende Format:

```
/vmfs/devices/disks/vmhbaA:T:L:0
```

Weitere Informationen finden Sie unter „vmkfstools-Befehlssyntax“ auf Seite 282.

Weitere Informationen zum Konfigurieren von RDM finden Sie unter „Raw-Device-Mapping“ auf Seite 151.

HINWEIS Alle Sperrmechanismen für VMFS-3-Dateien gelten auch für Raw-Festplatten-Zuordnungen.

Beispiel

vmkfstools -r /vmfs/devices/disks/vmhba1:3:0:0 foo_rdm.vmdk

Das Beispiel zeigt die Erstellung einer RDM-Datei mit dem Namen `foo_rdm.vmdk` und das Mapping der `vmhba1:3:0:0` Raw-Festplatte auf diese Datei. Sie können eine virtuelle Maschine so konfigurieren, dass sie die `foo_rdm.vmdk` Mapping-Datei verwendet, indem Sie die Konfigurationsdatei der virtuellen Maschine um die folgenden Zeilen ergänzen:

```
scsi0:0.present = TRUE
scsi0:0.fileName = /vmfs/volumes/myVMFS/foo_rdm.vmdk
```

Aufführen der Attribute eines RDM

`-q --queryrdm <rdm_Datei>`

Mit dieser Option können Sie die Attribute einer Raw-Festplatten-Zuordnung auflisten.

Bei Verwendung mit einer `RDM:<device>` oder `Raw:<device>` Angabe druckt diese Option den vmhba-Namen der Raw-Festplatte aus, auf die das `<device>` verweist, das diese Mapping-Datei verwendet. Diese Option druckt ebenfalls eine bestehende Identifizierungsinformation zur Raw-Festplatte aus.

Anlegen einer Raw Device Mapping-Datei im physischen Kompatibilitätsmodus

`-z --createrdmpassthru <Gerät>`

Mit dieser Option können Sie ein Pass-Through-Raw-Gerät zu einer Datei auf einem VMFS-Datenträger zuordnen. Mit dieser Form des Mappings kann eine virtuelle Maschine das ESX Server SCSI Befehlsfiltern umgehen, wenn sie auf ihre virtuelle Festplatte zugreift. Diese Art des Mappings eignet sich dann, wenn die virtuelle Maschine eigenständige SCSI-Befehle versenden muss, wie beispielsweise dann, wenn SAN-gestützte Software auf der virtuellen Maschine ausgeführt wird.

Wenn Sie diese Art der Zuordnung aktiviert haben, können Sie damit auf die Raw-Festplatte wie auf jede andere virtuelle Festplatte zugreifen.

Bei der Angabe des Werts für das `<Gerät>`, geben Sie `0` für die Partition an, was darauf hinweist, dass das gesamte Raw-Gerät verwenden wird. Verwenden Sie das folgende Format:

```
/vmfs/devices/disks/vmhbaA:T:L:0
```

Weitere Informationen finden Sie unter„vmkfstools-Befehlssyntax“ auf Seite 282.

Anlegen einer Deskriptor-Datei für ein Raw-Gerät

`-Q --createrawdevice <Gerät>`

Diese Option erstellt eine Raw-Geräte-Deskriptordatei auf einem VMFS-Datenträger. Diese Option sollte nur mit generischen SCSI-Geräten, wie z. B. Bandlaufwerken verwendet werden.

Verwenden Sie für den Parameter `<Gerät>` folgendes Format:

```
/vmfs/devices/generic/vmhbaA:T:L:P
```

Weitere Informationen finden Sie unter „vmkfstools-Befehlssyntax“ auf Seite 282.

Anzeige der Architektur der virtuellen Festplatte

`-g --geometry <Quelldatei>`

Mit dieser Option werden Informationen zur Architektur einer virtuellen Festplatte angezeigt.

Die Ausgabe erfolgt in dieser Form: `Geometrie-Informationen C/H/S`, wobei `C` für die Anzahl der Zylinder, `H` die Anzahl der Köpfe und `S` die Anzahl der Sektoren angibt.

HINWEIS Beim Import von virtuellen Festplatten von VMware Workstation auf ESX Server kann es zu Fehlermeldungen bezüglich Diskrepanzen in der Festplattengeometrie kommen. Eine Diskrepanz in der Festplattengeometrie kann auch die Ursache von Problemen beim Laden eines Gast-Betriebssystems oder bei der Ausführung einer neu erstellten virtuellen Maschine sein.

Geräteoptionen

Mit den Geräteoptionen können Sie Verwaltungsaufgaben für Ihre physischen Speichergeräte durchführen, mit denen Sie arbeiten. Sie können auch die meisten dieser Aufgaben auch über den VI Client ausführen.

In diesem Abschnitt werden folgende Themen behandelt:

- „Scan-Adapter“ auf Seite 294
- „Verwaltung der SCSI-Reservierungen von LUN“ auf Seite 294

Scan-Adapter

`–s ––scan<adapterName>`

Diese Option scannt einen bestimmten Adapter auf neu hinzugefügte oder geänderte Geräte oder LUNs. Die Option `-s` kann insbesondere für Adapter nützlich sein, die an Storage Area Networks (SANs) angeschlossen sind. Wenn ein neues Gerät oder eine neue LUN über einen Adapter neu zur Verfügung steht, registriert ESX Server dieses neue virtuelle Gerät zur Verwendung durch die virtuellen Maschinen. Wenn eine bestehende LUN nicht länger vorhanden ist, wird sie von der Liste der für die virtuellen Maschinen zur Verfügung stehenden Geräte entfernt.

Wenn Sie alle Adapter scannen möchten, verwenden Sie folgenden Befehl:

`esxcfg-rescan`

Sie können die Ergebnisse des Scans mit `ls /vmfs/devices/disks` anzeigen.

Beispiel

`vmkfstools –s vmhba1`

Dieses Beispiel zeigt den Scan des Adapters `vmhba1`, mit dem bestimmt wird, ob neue Ziele oder LUNs hinzugefügt wurden. Dieser Befehl stellt auch fest, wenn Ziele oder LUNs entfernt wurden.

Verwaltung der SCSI-Reservierungen von LUN

`–L ––lock [reserve|release|lunreset|targetreset|busreset] <Gerät>`

Mit dieser Option können Sie eine SCSI-LUN für die ausschließliche Verwendung durch einen ESX Server-Host reservieren, eine Reservierung aufheben, sodass andere Hosts auf die LUN zugreifen können, und eine Reservierung zurücksetzen, wodurch alle Reservierungen eines Ziels aufgehoben werden.

VORSICHT Eine Verwendung der Option `-L`kann den Betrieb der anderen Server auf dem Storage Area Network (SAN) beeinträchtigen. Verwenden Sie die Option `-L`nur zur Fehlerbehebung beim Clustering-Set-up.

Verwenden Sie diese Option nie auf eine LUN mit einem VMFS-Volume, es sei denn, VMware empfiehlt Ihnen ausdrücklich etwas Anderes.

Sie können die Option `-L` auf verschiedene Arten anwenden:

- `-L reserve` – Reserviert die angegebene LUN. Nach der Reservierung kann nur der Server, der diese LUN reserviert hatte, darauf zugreifen. Wenn andere Server versuchen, auf diese LUN zuzugreifen, erhalten Sie einen Reservierungsfehler.
- `-L release` – Hebt die Reservierung der angegebenen LUN auf. Alle anderen Server können wieder auf die LUN zugreifen.
- `-L lunreset` – Setzt die angegebene LUN zurück, indem jede Reservierung der LUN zurückgesetzt und die LUN den anderen Servern wieder zur Verfügung gestellt wird. Dies beeinflusst die anderen LUNs auf dem Gerät nicht. Wenn eine andere LUN auf dem Gerät reserviert wurde, bleibt sie reserviert.
- `-L targetreset` – Setzt das gesamte Target zurück. Dadurch werden die Reservierungen für alle LUNs, die dem Ziel zugeordnet sind, aufgehoben; die entsprechenden LUNs stehen wieder für alle Server zur Verfügung.
- `-L busreset` – Setzt alle zugänglichen Targets auf dem Bus zurück. Dadurch werden die Reservierungen für alle LUNs, auf die durch den Bus zugegriffen werden kann, aufgehoben; und die entsprechenden LUNs stehen wieder für alle Server zur Verfügung.

Verwenden Sie für den Parameter `<Gerät>` folgendes Format:

```
/vmfs/devices/disks/vmhbaA:T:L:P
```

Weitere Informationen finden Sie unter „vmkfstools-Befehlssyntax“ auf Seite 282.

Beispiele für die Verwendung von vmkfstools

In diesem Abschnitt finden Sie Beispiele für die Verwendung des Befehls `vmkfstools` mit den oben beschriebenen Optionen.

In diesem Abschnitt sind folgende Themen enthalten:

- „Anlegen eines neuen VMFS-3-Dateisystems“ auf Seite 295
- „Hinzufügen einer Partition zu einem VMFS-3-Dateisystem“ auf Seite 296
- „Neue virtuelle Festplatte erstellen“ auf Seite 296
- „Klonen einer virtuellen Festplatte“ auf Seite 296
- „Erstellen einer Raw-Device-Mapping“ auf Seite 296
- „Scannen eines Adapters auf Änderungen“ auf Seite 296

Anlegen eines neuen VMFS-3-Dateisystems

```
vmkfstools –C vmfs3 –b 1m –S myvmfs vmhba1:3:0:1
```

Dieses Beispiel zeigt die Erstellung eines neuen VMFS-3-Dateisystems mit dem Namen `myvmfs` auf der ersten Partition von Ziel 3, LUN 0 des SCSI-Adapters 1. Die Dateiblockgröße ist 1 MB.

Hinzufügen einer Partition zu einem VMFS-3-Dateisystem

```
vmkfstools –Z vmhba0:1:2:4 vmhba1:3:0:1
```

Dieses Beispiel zeigt die Erweiterung eines logischen Dateisystems durch das Hinzufügen einer neuen Partition. Das erweiterte Dateisystem nimmt nun zwei Partitionen ein – `vmhba1:3:0:1` und `vmhba0:1:2:4`. In diesem Beispiel ist `vmhba1:3:0:1` der Name der übergeordneten Partition.

Neue virtuelle Festplatte erstellen

```
vmkfstools –c 2048m /vmfs/volumes/myVMFS/myOS.vmdk
```

Dieses Beispiel zeigt die Erstellung einer virtuellen 2-GB-Festplattendatei mit dem Namen `myOS.vmdk` auf dem VMFS-Dateisystem mit dem Namen myVMFS. Diese Datei stellt eine leere virtuelle Festplatte dar, virtuelle Maschinen können darauf zugreifen.

Klonen einer virtuellen Festplatte

```
vmkfstools –i /vmfs/volumes/templates/gold–master.vmdk
              /vmfs/volumes/myVMFS/myOS.vmdk
```

Dieses Beispiel zeigt das Klonen der Inhalte einer virtuellen Master-Festplatte aus dem Vorlage-Repository auf eine virtuelle Festplattendatei mit der Bezeichnung `myOS.vmdk` auf dem Dateisystem mit der Bezeichnung `myVMFS`. Sie können die virtuelle Maschine so konfigurieren, dass diese virtuelle Festplatte verwendet wird, indem Sie die folgenden Zeilen zur Konfigurationsdatei der virtuellen Maschine hinzufügen:

```
scsi0:0.present = TRUE
scsi0:0.fileName = /vmfs/volumes/myVMFS/myOS.vmdk
```

Erstellen einer Raw-Device-Mapping

```
vmkfstools –r /vmfs/devices/disks/vmhba1:3:0:0 foo_rdm.vmdk
```

Das Beispiel zeigt die Erstellung einer RDM-Datei mit dem Namen `foo_rdm.vmdk` und das Mapping der `vmhba1:3:0:0` Raw-Festplatte auf diese Datei. Sie können eine virtuelle Maschine so konfigurieren, dass sie die Zuordnungsdatei `foo_rdm.vmdk` verwendet, wie auch im vorhergehenden Beispiel. Weitere Informationen finden Sie unter „Klonen einer virtuellen Festplatte“ auf Seite 296.

Scannen eines Adapters auf Änderungen

```
vmkfstools –s vmhba1
```

Dieses Beispiel zeigt den Scan des Adapters `vmhba1`, mit dem bestimmt wird, ob neue Ziele oder LUNs hinzugefügt wurden. Dieser Befehl stellt auch fest, wenn Ziele oder LUNs entfernt wurden.

Stichwortverzeichnis

Symbols

* neben dem Pfad **146**

A

Administratorrolle **218**

aktueller Multipathing-Status **145**

Ändern

- Anwender auf ESX Server-Hosts **223**
- Gruppen auf ESX Server-Hosts **226**
- Kennwortverwendungsdauer für Anwender oder Gruppen **246**
- Proxy-Dienste für ESX Server **230**
- Servicekonsolen-Kennwort-Plug-In **250**
- SSH-Konfiguration **256**

Änderung

- Kennwortverwendungsdauer für ESX Server **245**

Anwender

- Ändern auf ESX Server-Hosts **223**
- Anwender mit direktem Zugriff **214**
- Anwendertabelle für ESX Server-Hosts **220**
- Anzeige von Anwenderverzeichnissen **221**
- aus einer Windows-Domäne **214**
- Authentifizierung **214**
- Entfernen von ESX Server-Hosts **225**
- Export eines Anwenderverzeichnisses **221**
- Hinzufügen zu ESX Server-Hosts **222**
- VirtualCenter-Anwender **214**

Anwendergruppen

- Zugriff **14**

Anzeige von ESX Server-Host-Anwendern und -Gruppen **221**

Assistent zum Pfade verwalten **149**

Asterisk-Zeichen neben Pfad **146**

Authentifizieren

- Anwender **214**
- Gruppen **215**

Authentifizierungsdaemon **211**

B

Befehlsübersicht für ESX Server **275**

Bestimmung der Sicherheitsstufe der Firewall für die Servicekonsole **241**

bevorzugter Pfad **146**, **149**, **150**

Blade-Server

- Konfigurieren einer Protgruppe für virtuelle Maschinen **77**
- Konfigurieren eines VMkernel-Ports **78**
- und virtuelle Netzwerke **76**

Blockieren von Ports in der Servicekonsolen-Firewall **242**

C

CIM und Firewall-Ports **192**

D

DAS-Firewall-Port für ESX Server **187**
Datastores
- Anzeige im VI Client **93**
- Entfernen **139**
- Erstellung auf einer SCSI-Festplatte **104**
- Erstellung auf Fibre-Channel-Geräten **108**
- Erstellung auf hardware-initiiertem iSCSI-Speicher **120**
- Erstellung auf software-initiiertem iSCSI-Speicher **129**
- Hinzufügen von Erweiterungen **141**
- Konfiguration auf NFS-Datenträgern **135**
- neu scannen **131**
- Umbenennen **140**
- und Dateisysteme **90**
- Verwaltung **138**

Dateisysteme
- Aktualisierung **139**
- NFS **91**
- Verwaltung **138**
- VMFS **91**

Deaktivieren
- Authentifizierung für iSCSI-Adapter **207**
- Kopiervorgänge für Gastbetriebssysteme **266**
- Protokollierung für Gastbetriebssysteme **270**, **272**

Deaktivierung
- SSL für VI-Web Access und SDK **228**

Delegierter **234**
delegierter Anwender **235**
DHCP **43**
DNS **62**
dynamische Erkennung **112**

E

Einrichten der CHAP-Authentifizierung für iSCSI-Adapter **206**
Entfernen
- Anwender aus Gruppen **226**
- Anwender von ESX Server-Hosts **225**
- Gruppen von ESX Server-Hosts **227**

Erweiterungen **141**
ESX Server
- Ändern von Proxy-Diensten **230**
- Anwender **211**
- Architektur und Sicherheitsfunktionen **168**
- Authentifizierung **211**
- Authentifizierung für iSCSI-Speicher **204**
- Befehlsübersicht **275**
- Delegierter **234**
- Hinzufügen von Anwendern **222**
- Hinzufügen von Gruppen **225**
- Host-Host-Firewall-Ports **191**
- Implementierungen und Sicherheit **259**
- Kennwortbeschränkungen **244**
- Schlüsselqualität für Verbindungen **252**
- Sicherheit virtueller Switches **197**
- Sicherheitsübersicht **168**
- VLAN-Sicherheit **197**

ESX Server-Host-Kennwörter
Ändern des Plug-Ins **250**
Komplexität **246**
Konfiguration der Kennwort-Komplexität **249**
Konfiguration von Wiederverwendungsregeln **249**
neue Kennwortkriterien **246**
Verwendungsdauer **245**
esxcfg-Befehle **275**
EUI-Bezeichner **112**
Export von ESX Server-Host-Anwendern und -Gruppen **221**

F

Failover **57**
Failover-Pfade
Status **145**
Failovers
mit Fibre-Channel-Speicher **143**
Festlegung der Sicherheitsstufe der Servicekonsolen-Firewall **241**
Feststehende Pfadkonventionen **147**
bevorzugter Pfad **149**
Fibre-Channel-Speicher
Hinzufügen **108**
Übersicht **106**
Firewall-Ports
Backup-Agenten **240**
Bestimmung der Sicherheitsstufe der Firewall für die Servicekonsole **241**
CIM **192**
direkte Verbindung mit VI Client **185**
direkte Verbindung mit VI-Web Access **185**
Festlegung der Sicherheitsstufe der Servicekonsolen-Firewall **241**
Freigeben beim VI Client **192**
Freigeben und Blockieren für die Servicekonsole **242**
FTP **192**
für Management-Zugriff **187**
Host-Host **191**
iSCSI-Software-Client **192**
Konfiguration mit einem Virtual-Center-Server **182**
Konfiguration ohne VirtualCenter-Server **185**
Lizenz-Server und VirtualCenter-Server **182**
Management **192**
NFS **192**
NIS **192**
SDK und die Konsole der virtuellen Maschine **189**
Servicekonsole **240**
Sicherheitsstufe **240**
SMB **192**
SNMP **192**
SSH **192**
Übersicht **181**
und Verschlüsselung **228**
unterstützte Dienste **192**
VI Client und die Konsole der virtuellen Maschine **189**
VI Client und VirtualCenter-Server **182**
VI-Web Access und die Konsole der virtuellen Maschine **189**
VI-Web Access und VirtualCenter-Server **182**
zur Anbindung der Konsole der virtuellen Maschine **189**

Freigeben von Ports in der Servicekonsolen-Firewall **242**
FTP und Firewall-Ports **192**

G

Gastbetriebssysteme
- Deaktivierung der Protokollierung **270**, **272**
- Deaktivierung von Kopiervorgängen **266**
- Sicherheitsempfehlungen **265**

Gruppen
- Ändern auf ESX Server-Hosts **226**
- Anzeige von Gruppenverzeichnissen **221**
- Authentifizierung **215**
- Entfernen von ESX Server-Hosts **227**
- Export eines Gruppenverzeichnisses **221**
- Gruppentabelle für ESX Server-Hosts **220**
- Hinzufügen zu ESX Server-Hosts **225**

H

Hinzufügen
- Anwender zu ESX Server-Hosts **222**
- Anwender zu Gruppen **226**
- Fibre-Channel-Speicher **108**
- Gruppen zu ESX Server-Hosts **225**
- lokaler SCSI-Speicher **104**
- mittels Hardware ausgelöste iSCSI-Speicherung **120**
- NFS-Speicher **135**
- software-initiierter iSCSI-Speicher **129**

HTTP- und HTTPS-Firewall-Port **187**

I

IQN-Bezeichner **112**
iSCSI
- Authentifizierung **204**
- CHAP **204**
- Deaktivierung der Authentifizierung **207**
- Firewall-Port für ESX Server **187**
- Konfiguration der CHAP-Authentifizierung **206**
- Netzwerk **70**
- QLogic-iSCSI-Adapter **204**
- Schutz übertragender Daten **208**
- Sicherheit **204**
- Software-Client und Firewall-Ports **192**
- Überprüfung der Authentifizierung **205**

iSCSI Netzwerk
- Anlegen einer Servicekonsolen-Verbindung **74**
- Anlegen eines VMkernel-Ports **70**

iSCSI Speicher
- Initiatoren **110**

iSCSI-HBA
- Alias **116**
- CHAP-Authentifizierung **119**
- CHAP-Parameter **116**
- dynamische Erkennung **116**
- statische Erkennung **116**

iSCSI-Speicher
- Erkennung **112**
- EUI-Bezeichner **112**
- Hardware-initiiert **110**
- IQN-Bezeichner **112**
- Namenformate **112**

Sicherheit **113**
software-initiiert **110**
Isolierung
Virtuelle Maschine **168**
virtuelle Netzwerk-Layer **173**
virtuelle Switches **173**
VLANs **173**

K

kanonische Pfade **145**
Kennwortbeschränkungen
für den ESX Server-Host **244**
Komplexität **246**
Mindestlänge **246**
Verwendungsdauer **245**
Kompatibilitätsmodi
physisch **157**
virtuell **157**
Konfiguration
delegierter Anwender **235**
ESX Server-Zertifikatsuche **229**
Fibre-Channel-Speicher **108**
Kennwort-Komplexität **249**
lokaler SCSI-Speicher **104**
mittels Hardware ausgelöste iSCSI-Speicherung **120**
RDM **161**
software-initiierter iSCSI-Speicher **129**
Wiederverwendungsregeln von Kennwörtern **249**
Konfigurieren
Multipathing für Fibre-Channel-Speicher **147**

L

Lastausgleich **57**
Lizenz-Server
Firewall-Ports für **187**
Firewall-Ports mit VirtualCenter-Server **182**
lokaler SCSI-Speicher
Hinzufügen **104**
Übersicht **104**

M

MAC-Adresse
Generieren **65**
Konfiguration **66**
Management-Zugriff
Firewall-Ports **187**
mittels Hardware ausgelöste iSCSI-Speicherung
Hinzufügen **120**
Übersicht **113**
Multipathing
aktive Pfade **145**
ausgefallene Pfade **145**
Betriebsbereite Pfade **145**
deaktivierte Pfade **145**
Failover **147**
für Fibre-Channel-Speicher **143**
kanonische Pfade **145**
Verwalten **147**
Multipathing-Policy
Einstellung **147**
Multipathing-Status **145**

N

NAS
Einbindung **67**
Firewall-Port für ESX Server **187**
Nessus **257**
Netzwerke
Sicherheit **194**

Netzwerkempfehlungen **67**
NFS
Delegierter **234**
Firewall-Ports **192**
NFS-Speicher
Hinzufügen **135**
Übersicht **132**
NIC-Teambildung
Definition **22**
NIS und Firewall-Ports **192**

P

pam_cracklib.so-Plug-In **246**
pam_passwdqc.so-Plug-In **250**
Pfadausfall **143**
Pfade
aktiveren **149**
bevorzugt **146**, **149**, **150**
deaktivieren **149**
Pfade aktivieren **149**
Pfade deaktivieren **149**
Pfadkonventionen
Feststehend **147**
Zuletzt verwendet **147**
Port-Gruppe
Definition **22**
Konfigurieren **60**
Verwendung **26**
Portsicherung bei iSCSI **208**
Proxy-Dienste
Ändern **230**
und Verschlüsselung **228**

R

Raw Device Mapping
siehe RDM **152**
Raw-Device-Map (RDM)
und vmkfstools **164**
RDM
dynamische Namensauflösung **158**
Erstellung **161**
für Cluster **160**
physischer Kompatibilitätsmodus **157**
Übersicht **152**
und virtuelle Festplattendateien **160**
virtueller Kompatibilitätsmodus **157**
Vorteile **153**
Ressourcenbegrenzungen und Sicherheit **168**
Ressourcengarantien und Sicherheit **168**
Rolle Kein Zugriff **218**
Rolle Lesezugriff **218**
Rollen
Administrator **218**
Kein Zugriff **218**
Lesezugriff **218**
Standard **218**
und Berechtigungen **218**
Root-Anmeldung
SSH **255**
Zugriffsberechtigungen **216**
Root-log-in
Delegierter **234**
Routing **62**
RPMs **257**

S

Schutz vor böswilliger Gerätetrennung **268**
SCSI
vmkfstools **281**
SDK und Firewall-Ports zur Anbindung der Konsole der virtuellen Maschine **189**

Servicekonsole
Absicherung durch VLANs und virtuelle Switches **197**
Anmeldung **239**
direkte Verbindungen **239**
Kennwortbeschränkungen **244**
Remote-Verbindungen **239**
setgid-Anwendungen **252**
setuid-Anwendungen **252**
Sicherheit **171**
Sicherheitsempfehlungen **238**
SSH-Verbindungen **255**
Servicekonsolenvernetzung
Fehlerbehebung **80**
Konfiguration **37**
setgid-Anwendungen **252**
setuid-Anwendungen **252**
sichere Implementierungen **259**
Sicherheit
Abtast-Software **257**
Anwender mit direktem Zugriff **214**
Anwenderauthentifizierung **211**
Anwendermanagment **211**
Beispiel, DMZ auf einem ESX Server-Host **173**, **175**
CHAP-Authentifizierung **204**
Delegierter **234**
Empfehlungen für virtuelle Maschinen **265**
ESX Server-Architektur **168**
gefälschte Übertragungen **201**
Gruppen **215**
iSCSI-Speicher **204**
Kennwortbeschränkungen für den ESX Server-Host **244**
MAC-Adressänderungen **201**
PAM-Authentifizierung **211**
Patches **257**
Promiscuous-Modus **201**
Rollen **218**
Schlüsselqualität **252**
setgid-Anwendungen **252**
setuid-Anwendungen **252**
Sicherheitsmaßnahmen für die Servicekonsole **171**
Sicherheitsstufe der Servicekonsolen-Firewall **240**
Sicherheitszertifikate **228**
SSH-Verbindungen **255**
Übersicht über Anwender, Gruppen, Zugriffsberechtigungen und Rollen **213**
Verschlüsselung **228**
VirtualCenter-Anwender **214**
Virtualisierungs-Layer **168**
Virtuelle Maschinen **168**
Virtuelle Netzwerk-Layer **173**
Virtuelles Netzwerk **194**
VLAN-Hopping **197**
VLANs **194**
VMkernel **168**
vmware-authd **211**
VMware-Policy **179**
Zugriffsberechtigungen **216**
Sicherheit für Layer 2 **53**
SMB und Firewall-Ports **192**
SNMP und Firewall-Ports **192**
software-initiierter iSCSI-Speicher
Hinzufügen **129**
Übersicht **121**
Speicher
Absicherung durch VLANs und virtuelle Switches **197**
Adapter **92**

Anzeige im VI Client **93**
Fibre-Channel **106**
iSCSI **110**
Konfigurationsaufgaben **101**
Konzepte **88**
lokaler SCSI-Speicher **104**
Multipathing **143**
NFS **132**
SAN **106**
Typen **91**
Zugriff durch virtuelle Maschinen **92**
Speicheradapter
Anzeige im VI Client **95**
Fibre-Channel **106**
iSCSI-HBA **116**
neu scannen **131**
Speicherzugriff **92**
SSH
Ändern der Konfiguration **256**
Firewall-Ports **192**
Sicherheitseinstellungen **255**
statische Erkennung **112**

T

TCP-Ports **187**
Tomcat Web **171**
Traffic-Shaping **55**

U

Überprüfung der Authentifizierung für iSCSI-Adapter **205**
UDP-Ports **187**
Unterstützung von Drittanbieter-Software **179**

V

Vernetzung von virtuellen Maschinen **29**
Verschlüsselung
für Anwendernamen, Kennwörter und Pakete **228**
und S **228**
VI Client
Firewall-Ports für direkte Verbindungen **185**
Firewall-Ports mit VirtualCenter-Server **182**
Firewall-Ports zur Anbindung zur Konsole der virtuellen Maschine **189**
VirtualCenter-Server
Firewall-Ports **182**
Zugriffsberechtigungen **216**
Virtualisierungs-Layer und Sicherheit **168**
Virtuelle Maschinen
Deaktivierung von Kopiervorgängen **266**
Gerätetrennung verhindern **268**
Ressourcenreservierungen und Begrenzungen **168**
Sicherheit **168**
Sicherheitsempfehlungen **265**
virtuelle Maschinen
Anlegen eines delegierten Anwenders **235**
Beispiel für Isolierung **173**, **175**
Deaktivierung der Protokollierung **270**, **272**
Delegierter **234**
virtuelle Netzwerk-Layer und Sicherheit **173**
Virtuelle Switches
Sicherheit **199**
virtuelle Switches
Angriffe über 802.1Q- und ISL-Kennzeichnung **199**

doppelt eingekapselte Angriffe **199**
gefälschte Übertragungen **201**
Implementierungsszenarien **259**
MAC-Adressänderungen **201**
MAC-Flooding **199**
Multicast-Brute-Force-Angriffe **199**
Promiscuous-Modus **201**
Spanning-Tree-Angriffe **199**
und iSCSI **208**
Zufallsdatenblock-Angriffe **199**
VI-Web Access
Deaktivierung von SSL **228**
Firewall-Ports für die Anbindung der Konsole der virtuellen Maschine **189**
Firewall-Ports für direkte Verbindungen **185**
Firewall-Ports mit VirtualCenter-Server **182**
und ESX Server-Dienste **228**
VLAN
Definition **22**
VLANs
Implementierungsszenarien **259**
Layer-2-Sicherheit **197**
Sicherheit **194**
und iSCSI **208**
VLAN-Hopping **197**
VMFS
Freigabe **259**
vmkfstools **281**
VMkernel
Definition **22**
Konfiguration **33**
Sicherheit **168**
vmkfstools
Dateisystemoptionen **284**
Geräteoptionen **294**
Optionen für virtuelle Festplatten **287**
Syntax **282**
Übersicht **281**
Verwendungsbeispiele **295**
VMotion
Absicherung durch VLANs und virtuelle Speicher **197**
Definition **22**
Firewall-Port **187**
Netzwerkkonfiguration **33**
VMware Community-Foren
Zugriff **14**
vSwitch
Bearbeiten **46**
Definition **22**
Policys **53**
Verwendung **23**

W

Wissensbasis
Zugriff **14**

Z

Zertifikate
Deaktivierung von SSL für VI-Web Access und SDK **228**
Konfiguration der ESX Server-Suche **229**
Schlüsseldatei **228**
Speicherort **228**
Zertifikatdatei **228**
Zertifizierung **179**
Zugriffsberechtigun **216**
Zugriffsberechtigungen
Root-Anwender **216**
Übersicht **216**
und Zugriffsberechtigungen **216**

VirtualCenter-Administrator **216**
vpxuser **216**
Zuletzt verwendete
Pfadkonventionen **147**